INGRAM MICRO EYESIGHT

NETFORMERS OSINT SECURITY REPORT

www.example-domain.com

11 May 2021

confidential

INGRAM MICRO SECURITY

NETFORMERS Engineering Your Future

Document details

Document

Title	Eyesight Report
Subject	BERGER LEVRAULT
Target URL	www.example-domain.com

Document Version

Version	Date	Changes	Author (s)
0.1	11 May 2021	Initial Version	Aswin Gopalakrishnan
1.0	11 May 2021	Internally Reviewed Final Version	Sebastian Eitel, Brian Verburg, Hugo Inigo

Contact information

Name	TBD
Function	TBD
E-mail address	TBD

Disclaimer

Ingram Micro Cyber Security Center of Excellence ©.

NetFormers Cyber Security.

This document is provided by Ingram Micro and NetFormers Cyber Security Team and classified as confidential.

Executive Summary

The Cyber Security Center of Excellence of IngramMicro conducted a comprehensive public discovery report (PDR) of BERGER LEVRAULT by gathering data from public sources such as those available on the Internet. The intelligence information was gathered, analysed and converted into a human readable form, which was reviewed, and risks identified. The objective of this assessment is to provide the BERGER LEVRAULT management team an understanding of the domain information exposed to the public Internet.

Scope

The test scope for this engagement is: **www.example-domain.com**

Testing was performed on 11.May 2021. Additional days were utilized to produce the report.

Assessment was performed using industry-standard open source intelligence tools and frameworks, including Shodan, Censis.io, Fierce, Tidos Framework, the Google-Dorks, Alienware Threat intelligence, Recon-ng , theHarvester, Metagoofil, SpiderFoot, Recorded-Future and Maltego.

Limitations

It is not within the scope of this engagement to evaluate the security posture of the target. The primary objective is to gather relevant information about the domain that may be utilised by hackers for conducting cyber-attacks. None of the identified risks were exploited during this engagement; these risks should only be treated as plausible threats with a likelihood of causing damage to the organisation.

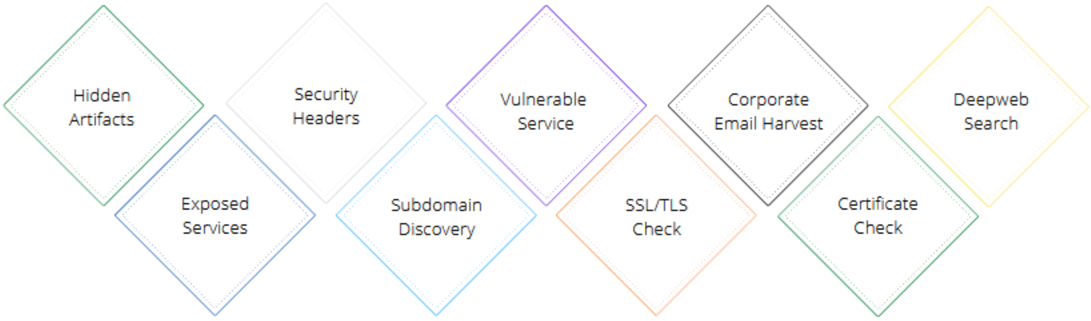
The findings in the report are not conclusive, as the results are generated automatically using a collection of industry-standard open source intelligence (OSINT) tools and frameworks. For more conclusive and thorough investigation of the domain or network, refer to other Cyber Security Service offerings of Ingram Micro. For more information, please reach out to your channel partner.

Methodology

The intelligence information gathered from publicly available resources are evaluated to identify risks and threats on any given target. These resources include search engines, paste sites, blogs, social networking sites, metadata and digital files, dark web resources geolocation, and anything available in the public internet.

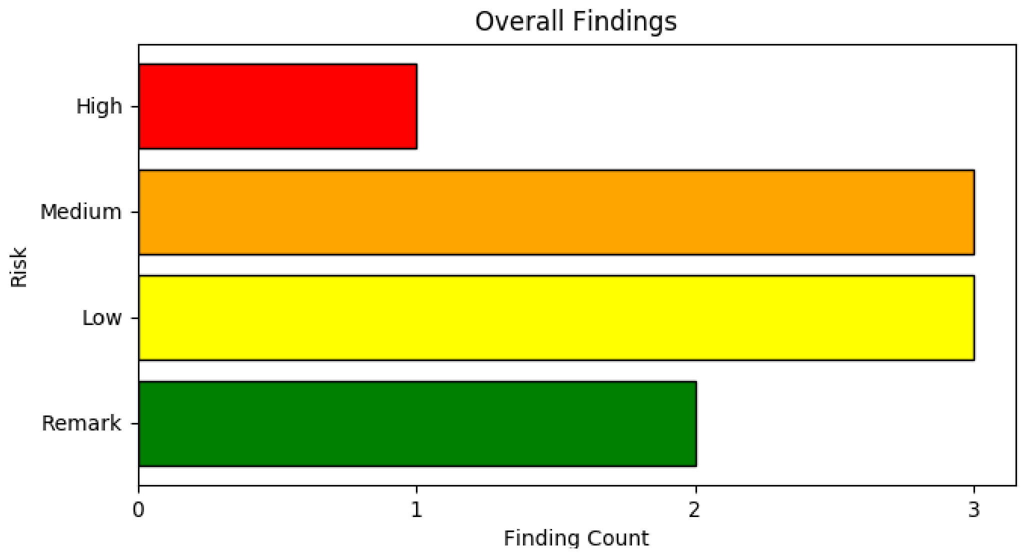
The PDR (aka OSINT) assessment distinguishes from other form of assessments because the collected information is legally accessible to the public without breach of any copyright or privacy laws. Therefore, the information accumulated, and methodologies used retrieve them strictly adhere to the legal and compliance regulations at Ingram Micro, and pose no risk to the customer's systems or information.

The image below describes the tactical intelligence gathered in this report:



Outcome

The following provide an overview of the findings identified during the engagement.



Since the business impact is hard to evaluate by us, all findings and their corresponding risks must be interpreted by Example-domain in the context of the system.

The outcome of the Eyesight investigation is below:

High finding one: The outdated software hosted the target has a public exploit available on the internet. This provides an entry point to the hackers, as they do not need to develop new exploit to breach the system, instead they can use the existing and focus more on creating a sophisticated payload that is harder to detect. This risk affects confidentiality, integrity and availability of the application.

Medium finding one: Few corporate email accounts were found in the database of hacked websites and leaked passwords. An attacker can use the compromised accounts for a variety of purposes including spam, phishing, fraud, and identity theft attacks. The risk affects the confidentiality of user data.

Medium finding two: The application server does not enforce have all the relevant security headers to protect modern browsers from encountering vulnerabilities. These headers act as the first layer of security to help mitigate certain types of attacks. These findings impact confidentiality, integrity and availability of data.

Medium finding three: Expired certificate does not offer any protection to the customer data. Expired certificates produce scary browser warning that drives customers due to the fear that the website does not secure their credentials. Both brand reputation and customer trust are damaged here. The risk affects confidentiality and Integrity of user data.

Low finding one: Open ports increase the risk of a data breach as these are doorways to the organisation's secure perimeter. An attacker may exploit the services hosted on these ports and gain access to the internal network of the organisation.

Low finding two: The response from the domain server contains sensitive information about the installed technologies. This information may be used by an attacker to search for known or common misconfiguration that would assist in more complex cyber-attacks.

Low finding three: Using depreciated protocols places the integrity of the data at risk. An attacker may be able to modify, replay or reorder data without being detected by the receiving endpoint.

Technical Findings

- **Sensitive Exposed Ports:** Each exposed port to the public internet is a front door for the attacker to try and infiltrate. During reconnaissance, certain services were identified that were publicly accessible which may be unused by the application. When legitimate services are exposed to the public internet, these may be exploited through code execution or miss-configurations.

- **Breached Email Accounts:** Some of the corporate email accounts were found in the database of hacked websites and leaked passwords. This may be serious consequences as the Cyber-Criminals could take control of breached account email account and send fraudulent emails to known contacts and steal their personal and financial information.
- **Service Information Disclosure:** The HTTP response header(s) disclose information about the installed technologies on the server. This type of issues is non-exploitable in most cases and considered as web application security issues that allow attackers to gather information about the application server which can be used later in the attack lifecycle.
- **Missing Security headers:** The security headers are fundamental to the development of a web application as these protect against attacks which most websites are vulnerable such as Cross-Site-Scripting (XSS), code injection, click-jacking, etc.
- **Expired SSL/TLS Certificate:** Certificate seems to have been expired on services of the domain. This puts the personal information of the customers at risk especially when sensitive operations such as financial transaction are carried out. This can also result in decline in sales and revenue as customers do not trust site anymore.
- **Outdated Software:** There are technologies installed on the server which were identified as outdated and have vulnerabilities. If there are known exploits in exploit databases(or deep web) for these vulnerabilities, an attacker may leverage them and gain access to the organisation network.
  - The software hosted on TCP port 4443 in host IP XX.XX.20.134 is running an outdated software Apache httpd
  - The software hosted on TCP port 443 in host IP XX.XX.29.10 is running an outdated software Microsoft IIS httpd 7.5
- **SSL/TLS Version:** The target domain uses outdated cypher suites that are often vulnerable to attacks. These protocols may be affected by vulnerabilities such as FREAK, POODLE, BEAST, and CRIME. If you must still support TLS 1.0, disable TLS 1.0 compression to avoid CRIME attacks.

Technical Recommendation

- **Sensitive Exposed Ports:** Opening ports to public internet should be on a "need-to-be" basis. Implement continuous monitoring technologies to identify risks in these open ports.
- **Breached Email Accounts:** Check and update your computer’s security. Use the latest Endpoint Security software and update its malware database regularly. Further, enforce strong password policies in the corporate network. Use added security features like Multi-Factor authentication to addition login security. Enforce Password-Rotations every two months. Lastly, refrain from clicking on links without validating its legitimacy.
- **Service Information Disclosure:** Configure the technologies such that their headers or messages (success or error) do not disclose information regarding their version and properties.
- **Missing Security headers:** Enforce the relevant security headers by default, unless there are overriding concerns in which case, such specific headers should be removed or modified.
- **Expired SSL/TLS Certificate:** Renew certificate from reputed certificate authorities to ensure trust from the customers.
- **Outdated Software:** Update the relevant technology to the latest version or install the necessary patch to fix the vulnerability. If there are dependencies on legacy application or libraries, install industry-recommended endpoint security solutions to detect and prevent attacks.
- **SSL/TLS Version:** Use modern cryptographic cypher suites and algorithms with desirable performance and security properties TLS/SSL protocols-based attacks.

Investigation

This chapter lays out the information gathering that was performed regarding www.example-domain.com's internet-facing infrastructure. More information sources were queried than reported in this chapter; sources that did not yield relevant information were left out.

HTTP Headers

A great deal of information can be gathered in a check of the HTTP Headers from a web server. Server-side software can be identified often down to the exact version running. Cookie strings, web application technologies and other data can be gathered from the HTTP Header. This information can be used when troubleshooting or when planning an attack against the web server.

HTTP Header Info

```
HTTP/1.1 301 Moved Permanently
Content-length: 0
Location: https://www.example-domain.com/
Connection: close

HTTP/1.1 302 Found
Date: Tue, 11 May 2021 13:29:10 GMT
Server: Apache
Location: https://www.example-domain.com/ca/en/
Cache-Control: max-age=0
Expires: Tue, 11 May 2021 13:29:10 GMT
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Vary: Accept-Encoding
Content-Length: 0
Content-Type: text/html; charset=UTF-8
X-XSS-Protection: 1;mode=block
Strict-Transport-Security: max-age=63072000

HTTP/1.1 200 OK
Date: Tue, 11 May 2021 13:29:10 GMT
Server: Apache
Last-Modified: Fri, 07 May 2021 15:27:20 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=0
Expires: Tue, 11 May 2021 13:29:10 GMT
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Content-Length: 20883
Content-Type: text/html; charset=UTF-8
X-XSS-Protection: 1;mode=block
Strict-Transport-Security: max-age=63072000
```

The following information was identified from the web server

- Server (Apache)

Finding 1: The HTTP response header(s) disclose information on the installed technology. An attacker can use that information to research vulnerabilities in those technologies to attack the application and breach the system.
[Severity of this risk: LOW]

These HTTP responses were inspected to identify the various security header implemented on the web application. These headers prevent modern browsers from running into easily preventable vulnerabilities.

These following security headers were missing from web application response:

- Content-Security-Policy: Offers an added layer of protection that help mitigate certain types of attacks, such as Cross Site Scripting (XSS) and data injection attacks. Such attacks are often used for data theft, site defacement and malware distribution.
- X-Permitted-Cross-Domain-Policies: Enforces the cross-domain policies which client like Flash and Adobe could use. This is to prevent Flash and Adobe Acrobat from loading content from one's domain from another website which may lead to unexpected data disclosure.
- Referrer-Policy: Controls how much referrer information should be included with the request. Flags such as "no-referrer" ensures that no referrer information is sent along a request.
- Expect-CT: Allows sites to report or enforce Certificate transparency requirements to prevent the use of miss-issued certificates for that site from going unnoticed.

Finding 2: The security headers are fundamental to the development of a web application as these protect against attacks which most websites are vulnerable such as Cross-Site-Scripting(XSS), code injection, click-jacking, etc.
[Severity of this risk: MEDIUM]

Discoverable Links

The section displays the links of the website from all public sources.

Links
https://www.example-domain.com/ca/en/
https://www.example-domain.com/ca/en/example-domain-group/
https://www.example-domain.com/ca/en/insight/
https://www.example-domain.com/ca/en/working-at-example-domain/
https://www.example-domain.com/ca/en/newsroom/
https://www.example-domain.com/ca/en/contact-us/
https://www.example-domain.com/ca/en/access-your-client-area/
https://www.example-domain.com/
https://www.example-domain.com/fr/
https://www.example-domain.com/ma/
https://www.example-domain.com/es/
https://www.example-domain.com/ca/en/
https://www.example-domain.com/ca/fr/
https://www.example-domain.com/ca/en/example-domain-group/
https://www.example-domain.com/ca/en/example-domain-group/who-are-we/
https://www.example-domain.com/ca/en/example-domain-group/worldwide-presence/all/
https://www.example-domain.com/ca/en/example-domain-group/our-history-from-1463/
https://www.example-domain.com/ca/en/example-domain-group/commitments/
https://www.example-domain.com/ca/en/example-domain-group/bl-institute/
https://www.example-domain.com/ca/en/example-domain-group/partners/
https://www.example-domain.com/ca/en/example-domain-group/bl-institute/
https://www.example-domain.com/ca/en/working-at-example-domain/
https://www.example-domain.com/ca/en/working-at-example-domain/job-and-internship-openings/
https://www.example-domain.com/ca/en/working-at-example-domain/
https://www.example-domain.com/ca/en/working-at-example-domain/our-hiring-vision/
https://www.example-domain.com/ca/en/working-at-example-domain/empower-talent/
https://www.example-domain.com/ca/en/working-at-example-domain/relations-with-universities-and-colleges/
https://www.example-domain.com/ca/en/?page_id=3724
https://www.example-domain.com/ca/en/example-domain-group/
https://www.example-domain.com/ca/en/insight/

https://www.example-domain.com/ca/en/working-at-example-domain/

https://www.example-domain.com/ca/en/newsroom/

https://www.example-domain.com/ca/en/contact-us/

https://www.example-domain.com/ca/en/access-your-client-area/

https://www.example-domain.com/ca/en/example-domain-group/who-are-we/

https://www.example-domain.com/ca/en/example-domain-group/worldwide-presence/all/

https://www.example-domain.com/ca/en/example-domain-group/our-history-from-1463/

https://www.example-domain.com/ca/en/example-domain-group/commitments/

https://www.example-domain.com/ca/en/example-domain-group/bl-institute/

https://www.example-domain.com/ca/en/example-domain-group/partners/

https://www.example-domain.com/ca/en/example-domain-group/bl-institute/

https://www.example-domain.com/ca/en/working-at-example-domain/job-and-internship-openings/

https://www.example-domain.com/ca/en/working-at-example-domain/

https://www.example-domain.com/ca/en/working-at-example-domain/our-hiring-vision/

https://www.example-domain.com/ca/en/working-at-example-domain/empower-talent/

https://www.example-domain.com/ca/en/working-at-example-domain/relations-with-universities-and-colleges/

https://www.example-domain.com/ca/en/?page_id=3724

https://www.example-domain.com/ca/en/software-and-solutions/

https://www.example-domain.com/ca/en/market/municipal-sector-and-public-administrations/

https://www.example-domain.com/ca/en/market/education-k-12-elementary-and-secondary-levels/

https://www.example-domain.com/ca/en/market/education-higher-education/

https://www.example-domain.com/ca/en/market/business/

https://www.example-domain.com/ca/en/customized-support-services/

https://www.example-domain.com/ca/en/all-products/markets/all/types/all/categories/all/subcategories/all/

https://www.example-domain.com/ca/en/category/management/rh-and-payroll/

https://www.example-domain.com/ca/en/category/management/finances-en/

https://www.example-domain.com/ca/en/category/management/taxation-en/

https://www.example-domain.com/ca/en/category/management/investments/

https://www.example-domain.com/ca/en/category/maintenance-en/cmms-asset-management-eam/

https://www.example-domain.com/ca/en/category/education-en/pedagogical-management/

https://www.example-domain.com/ca/en/category/management/registration-and-subscription-management/

https://www.example-domain.com/ca/en/category/education-en/schedule-and-premises-management/

https://www.example-domain.com/ca/en/product/hr-payroll-software-sofe/

https://www.example-domain.com/ca/en/product/time-management-software-sofe/

https://www.example-domain.com/ca/en/product/hr-payroll-software-coba/

https://www.example-domain.com/ca/en/product/financial-software-coba/

https://www.example-domain.com/ca/en/product/financial-software-sofe/

https://www.example-domain.com/ca/en/product/capital-assets-software-sofe/

https://www.example-domain.com/ca/en/product/municipal-taxation-software-sofe/

https://www.example-domain.com/ca/en/product/investment-software-sofe/

https://www.example-domain.com/ca/en/product/cmms-software-carl-source/

https://www.example-domain.com/ca/en/product/mobile-app-cmms-carl-touch/

https://www.example-domain.com/ca/en/product/service-requests-management-mobile-app-carl-flash/

https://www.example-domain.com/ca/en/product/cartographic-asset-representation-carl-maps/

https://www.example-domain.com/ca/en/product/internet-of-things-platform-carl-iot/

https://www.example-domain.com/ca/en/product/k-12-pedagogical-management-software-coba/

https://www.example-domain.com/ca/en/product/college-educational-management-software-coba/

https://www.example-domain.com/ca/en/product/activity-management-software-coba/

https://www.example-domain.com/ca/en/product/course-scheduling-software-infosilem-academic/

https://www.example-domain.com/ca/en/product/event-scheduling-software-infosilem-campus/

https://www.example-domain.com/ca/en/product/exam-scheduling-software-infosilem-exam/

https://www.example-domain.com/ca/en/product/student-scheduling-software-infosilem-sectioner/

https://www.example-domain.com/ca/en/product/hosting-service/

https://www.example-domain.com/ca/en/product/continuity-of-service-and-security/

https://www.example-domain.com/ca/en/software-and-solutions/

https://www.example-domain.com/ca/en/customized-support-services/

https://www.example-domain.com/ca/en/market/municipal-sector-and-public-administrations/

https://www.example-domain.com/ca/en/market/education-k-12-elementary-and-secondary-levels/

https://www.example-domain.com/ca/en/market/education-higher-education/

https://www.example-domain.com/ca/en/market/business/

https://www.example-domain.com/ca/en/all-products/markets/all/types/all/categories/all/subcategories/all/

https://www.example-domain.com/ca/en/category/management/rh-and-payroll/

https://www.example-domain.com/ca/en/category/management/finances-en/

https://www.example-domain.com/ca/en/category/management/taxation-en/

https://www.example-domain.com/ca/en/category/management/investments/

https://www.example-domain.com/ca/en/category/maintenance-en/cmms-asset-management-eam/

https://www.example-domain.com/ca/en/category/education-en/pedagogical-management/

https://www.example-domain.com/ca/en/category/management/registration-and-subscription-management/

https://www.example-domain.com/ca/en/category/education-en/schedule-and-premises-management/

https://www.example-domain.com/ca/en/product/hr-payroll-software-sofe/

https://www.example-domain.com/ca/en/product/time-management-software-sofe/

https://www.example-domain.com/ca/en/product/hr-payroll-software-coba/

https://www.example-domain.com/ca/en/product/financial-software-coba/

https://www.example-domain.com/ca/en/product/financial-software-sofe/

https://www.example-domain.com/ca/en/product/capital-assets-software-sofe/

https://www.example-domain.com/ca/en/product/municipal-taxation-software-sofe/

https://www.example-domain.com/ca/en/product/investment-software-sofe/

https://www.example-domain.com/ca/en/product/cmms-software-carl-source/

https://www.example-domain.com/ca/en/product/mobile-app-cmms-carl-touch/

https://www.example-domain.com/ca/en/product/service-requests-management-mobile-app-carl-flash/

https://www.example-domain.com/ca/en/product/cartographic-asset-representation-carl-maps/

https://www.example-domain.com/ca/en/product/internet-of-things-platform-carl-iot/

https://www.example-domain.com/ca/en/product/k-12-pedagogical-management-software-coba/

https://www.example-domain.com/ca/en/product/college-educational-management-software-coba/

https://www.example-domain.com/ca/en/product/activity-management-software-coba/

https://www.example-domain.com/ca/en/product/course-scheduling-software-infosilem-academic/

https://www.example-domain.com/ca/en/product/event-scheduling-software-infosilem-campus/

https://www.example-domain.com/ca/en/product/exam-scheduling-software-infosilem-exam/

https://www.example-domain.com/ca/en/product/student-scheduling-software-infosilem-sectioner/

https://www.example-domain.com/ca/en/product/hosting-service/

https://www.example-domain.com/ca/en/product/continuity-of-service-and-security/

https://www.example-domain.com/ca/en/product/course-scheduling-software-infosilem-academic/

https://www.example-domain.com/ca/en/product/course-scheduling-software-infosilem-academic/

https://www.example-domain.com/ca/en/working-at-example-domain/

https://www.example-domain.com/ca/en/working-at-example-domain/

https://www.example-domain.com/ca/en/product/hr-payroll-software-sofe/

https://www.example-domain.com/ca/en/product/hr-payroll-software-sofe/

https://www.example-domain.com/ca/en/product/event-scheduling-software-infosilem-campus/

https://www.example-domain.com/ca/en/product/event-scheduling-software-infosilem-campus/

https://www.example-domain.com/ca/en/product/municipal-taxation-software-sofe/

https://www.example-domain.com/ca/en/product/municipal-taxation-software-sofe/

https://www.example-domain.com/ca/en/product/cmms-software-carl-source/

https://www.example-domain.com/ca/en/product/cmms-software-carl-source/

https://www.example-domain.com/ca/en/product/college-educational-management-software-coba/
https://www.example-domain.com/ca/en/product/college-educational-management-software-coba/
https://www.example-domain.com/ca/en/product/k-12-pedagogical-management-software-coba/
https://www.example-domain.com/ca/en/product/k-12-pedagogical-management-software-coba/
https://www.example-domain.com/ca/en/all-products/markets/all/types/all/categories/all/subcategories/all/
https://www.example-domain.com/ca/en/all-products/markets/all/types/all/categories/all/subcategories/all/
https://www.example-domain.com/ca/en/example-domain-group/
https://www.example-domain.com/ca/en/insight/choosing-an-erp-system/
https://www.example-domain.com/ca/en/insight/choosing-an-erp-system/
https://www.example-domain.com/ca/en/insight/example-domain-adopts-the-slow-tech-attitude/
https://www.example-domain.com/ca/en/insight/example-domain-adopts-the-slow-tech-attitude/
https://www.example-domain.com/ca/en/insight/example-domain-supports-cities-to-reach-new-horizons/
https://www.example-domain.com/ca/en/insight/example-domain-supports-cities-to-reach-new-horizons/
https://www.example-domain.com/ca/en/insight/
https://www.example-domain.com/ca/en/news/ellucian-live-2021/
https://www.example-domain.com/ca/en/news/ellucian-live-2021/
https://www.example-domain.com/ca/en/news/looking-back-at-our-winter-events-2021/
https://www.example-domain.com/ca/en/news/looking-back-at-our-winter-events-2021/
https://www.example-domain.com/ca/en/news/5th-edition-of-the-cityzen-challenge-inter-school-contest/
https://www.example-domain.com/ca/en/news/5th-edition-of-the-cityzen-challenge-inter-school-contest/
https://www.example-domain.com/ca/en/newsroom/all-news/markets/all/categories/all/subcategories/all/calendar/all/
https://www.example-domain.com/ca/en/
https://www.example-domain.com/ca/en/legal-notices/
https://www.example-domain.com/ca/en/contact-us/
https://www.example-domain.com/ca/en/legal-notices/
https://www.example-domain.com/ca/en/browsing-help-and-accessibility-example-domain/
https://www.example-domain.com/ca/en/privacy-policy/
https://www.example-domain.com/ca/en/sitemap/

Remark: The severity of disclosed link is best realised by the organisation. The results are included as point of interest.
[Severity: Remark]

Organisation Email Addresses

The section displays domain specific emails addresses gathered from public sources. Organisational email addresses are often subjected to phishing attacks, which helps an attacker gain foothold in their internal network.

Email Addresses
sandra.hertz-moreno@example-domain.com
julien.nessi@example-domain.com
emilie.martin@example-domain.com
javier.jimenez@example-domain.com
guy.beaudet@example-domain.com
nathalie.veuillotte@example-domain.com
courrier@example-domain.com
maryse.penen@example-domain.com
stephanie.rey@example-domain.com
antonia.moreno@example-domain.com

vanessa-caron@example-domain.com
comunicacion.es@example-domain.com
ventes.canada@example-domain.com
communication@example-domain.com
dpo@example-domain.com
bl.institut@example-domain.com
olivier.evene@example-domain.com
commercial@example-domain.com
jimmy.benoits@example-domain.com
dpd@example-domain.com
fondation@example-domain.com
websitehelp@example-domain.com
relationclient@example-domain.com
resurgences_espace-clients@example-domain.com
christophe.bortolaso@example-domain.com
robotformeloqua@example-domain.com
info.carl@example-domain.com
el-ghazi.mountich@example-domain.com
infocanada@example-domain.com
alexia.decaix@example-domain.com
notifica@example-domain.com
ca.martineau@example-domain.com
jean-philippe.lente@example-domain.com
celia.picard@example-domain.com
valerie.reiner@example-domain.com

The gathered email addresses were further verified by checking against hacked and breached databases. The following was found:

Email Addresses	Breach Database
julien.nessi@example-domain.com	Apollo
emilie.martin@example-domain.com	Apollo
guy.beaudet@example-domain.com	Apollo, Cit0day
maryse.penen@example-domain.com	Apollo
stephanie.rey@example-domain.com	Apollo
olivier.evene@example-domain.com	Apollo
alexia.decaix@example-domain.com	Cit0day
ca.martineau@example-domain.com	Apollo
jean-philippe.lente@example-domain.com	Apollo, Nitro
valerie.reiner@example-domain.com	db8151dd

Note that certain sources may be marked as "Sensitive Source". This is because revealing the source may compromise an on-going investigation or the affected site is of a controversial nature.

For more information on the above listed breaches, refer to Appendix B: Known Breaches

It is imperative to understand how the email addresses were compromised. This is likely to happen in few ways:

- The software security in place is not up-to-date.
- A weak password policy is in place, which was easily cracked, or brute forced.
- Vulnerable to social engineering attack. An unsuspecting user may click on a malicious link in an email, IM conversation, or on a social engineering site, or webpage.
- Insufficient security enforcements like password rotation or Multi-Factor Authentications.

Finding 3: Some of the corporate email accounts were found in the database of hacked websites and leaked passwords. This may be serious consequences as the Cyber-Criminals could take control of breached account email account and send fraudulent emails to known contacts and steal their personal and financial information.
[Severity of this risk: MEDIUM]

Reverse DNS for Subdomain Enumeration

Reverse DNS helps discover the domain name associated with an IP Address by returning its PTR Record. This is one of the common techniques used by attacker to build organisation footprint.

Domain	IP Address
sfdc.example-domain.com	XX.XX.37.101
whoami2.pic.example-domain.com	XX.XX.37.101
whoami3.pic.example-domain.com	XX.XX.37.101
gitlab.pic.example-domain.com	XX.XX.37.101
passbold.pic.example-domain.com	XX.XX.37.101
sonarqube.pic.example-domain.com	XX.XX.37.101
mailhog.pic.example-domain.com	XX.XX.37.101
whoami.pic.example-domain.com	XX.XX.37.101
pj.pic.example-domain.com	XX.XX.37.101
traefik.pic.example-domain.com	XX.XX.37.101
lam.pic.example-domain.com	XX.XX.37.101
prometheus-system.pic.example-domain.com	XX.XX.37.101
bitwarden.pic.example-domain.com	XX.XX.37.101
iq-admin.pic.example-domain.com	XX.XX.37.101
phpldapadmin.pic.example-domain.com	XX.XX.37.101
pjson.pic.example-domain.com	XX.XX.37.101
nexusldap.pic.example-domain.com	XX.XX.37.101
registryldap.pic.example-domain.com	XX.XX.37.101
iq.pic.example-domain.com	XX.XX.37.101
registry-manager.pic.example-domain.com	XX.XX.37.101
docker.pic.example-domain.com	XX.XX.37.101
portainer.pic.example-domain.com	XX.XX.37.101
adminer.pic.example-domain.com	XX.XX.37.101
mailhog.libreair.pic.example-domain.com	XX.XX.37.101
usager.libreair.pic.example-domain.com	XX.XX.37.101
aws.libreair.pic.example-domain.com	XX.XX.37.101
jenkins.pic.example-domain.com	XX.XX.37.101
prometheus.pic.example-domain.com	XX.XX.37.101
nexus.pic.example-domain.com	XX.XX.37.101
communeit.pic.example-domain.com	XX.XX.37.101
swarmpit.pic.example-domain.com	XX.XX.37.101
gru.pic.example-domain.com	XX.XX.37.101
registry.pic.example-domain.com	XX.XX.37.101
blauth-preprod.example-domain.com	XX.XX.37.101
blat-preprod.example-domain.com	XX.XX.37.101
citizenconnect-preprod.example-domain.com	XX.XX.37.101
blgfpreprod.example-domain.com	XX.XX.37.101
blrhpreprod.example-domain.com	XX.XX.37.101
blenfance.example-domain.com	XX.XX.37.101
ge.example-domain.com	XX.XX.37.101
portail-labege.example-domain.com	XX.XX.37.101
gitlab.forge.example-domain.com	XX.XX.37.101
sonarqube.forge.example-domain.com	XX.XX.37.101
runner-cache.forge.example-domain.com	XX.XX.37.101
runners-cache.forge.example-domain.com	XX.XX.37.101

pje.forge.example-domain.com	XX.XX.37.101
traefik.forge.example-domain.com	XX.XX.37.101
prometheus-system.forge.example-domain.com	XX.XX.37.101
minio.forge.example-domain.com	XX.XX.37.101
nexus.minio.forge.example-domain.com	XX.XX.37.101
portainer.forge.example-domain.com	XX.XX.37.101
adminer.forge.example-domain.com	XX.XX.37.101
atlantis.forge.example-domain.com	XX.XX.37.101
runatlantis.forge.example-domain.com	XX.XX.37.101
jenkins.forge.example-domain.com	XX.XX.37.101
prometheus.forge.example-domain.com	XX.XX.37.101
nexus.forge.example-domain.com	XX.XX.37.101
swarmpit.forge.example-domain.com	XX.XX.37.101
registry.forge.example-domain.com	XX.XX.37.101
saas.ms.example-domain.com	XX.XX.37.101
test.ms.example-domain.com	XX.XX.37.101
blat.example-domain.com	XX.XX.37.101
citizenconnect.example-domain.com	XX.XX.37.101
cabinetnumeriqueaudit.example-domain.com	XX.XX.37.101
blbot.example-domain.com	XX.XX.37.101
portail-test.example-domain.com	XX.XX.37.101
whoami.forgetest.example-domain.com	XX.XX.225.1
traefik.forgetest.example-domain.com	XX.XX.37.101
portainer.forgetest.example-domain.com	XX.XX.37.101
swarmpit.forgetest.example-domain.com	XX.XX.37.101
cabinetnumeriquetest.example-domain.com	XX.XX.37.101
my-electiontest.example-domain.com	XX.XX.37.101
mail.cabinetdeselustest.example-domain.com	XX.XX.37.101
blog.workshops.gru.example-domain.com	XX.XX.37.101
app10.demo.workshops.gru.example-domain.com	XX.XX.37.101
s10.demo.workshops.gru.example-domain.com	XX.XX.37.101
app1.demo.workshops.gru.example-domain.com	XX.XX.37.101
s1.demo.workshops.gru.example-domain.com	XX.XX.37.101
app2.demo.workshops.gru.example-domain.com	XX.XX.37.101
s2.demo.workshops.gru.example-domain.com	XX.XX.37.101
app3.demo.workshops.gru.example-domain.com	XX.XX.37.101
s3.demo.workshops.gru.example-domain.com	XX.XX.37.101
app4.demo.workshops.gru.example-domain.com	XX.XX.37.101
s4.demo.workshops.gru.example-domain.com	XX.XX.37.101
app5.demo.workshops.gru.example-domain.com	XX.XX.37.101
s5.demo.workshops.gru.example-domain.com	XX.XX.37.101
app6.demo.workshops.gru.example-domain.com	XX.XX.37.101
s6.demo.workshops.gru.example-domain.com	XX.XX.37.101
s7.demo.workshops.gru.example-domain.com	XX.XX.37.101
app8.demo.workshops.gru.example-domain.com	XX.XX.37.101
s8.demo.workshops.gru.example-domain.com	XX.XX.37.101
app9.demo.workshops.gru.example-domain.com	XX.XX.37.101
showcase.demo.workshops.gru.example-domain.com	XX.XX.37.101
api.demo.workshops.gru.example-domain.com	XX.XX.37.101
admin.demo.workshops.gru.example-domain.com	XX.XX.37.101
backstage.cluster.workshops.gru.example-domain.com	XX.XX.37.101
kube-scale.cluster.workshops.gru.example-domain.com	XX.XX.37.101

mailhog.cluster.workshops.gru.example-domain.com	XX.XX.81.82
keycloak.cluster.workshops.gru.example-domain.com	XX.XX.81.82
check.cluster.workshops.gru.example-domain.com	XX.XX.81.82
heimdall.cluster.workshops.gru.example-domain.com	XX.XX.81.82
argo.cluster.workshops.gru.example-domain.com	XX.XX.81.82
rabbitmq.cluster.workshops.gru.example-domain.com	XX.XX.81.82
rancher.cluster.workshops.gru.example-domain.com	XX.XX.81.82
harbor.cluster.workshops.gru.example-domain.com	XX.XX.81.82
notary-harbor.cluster.workshops.gru.example-domain.com	XX.XX.81.82
nexus.cluster.workshops.gru.example-domain.com	XX.XX.81.82
container.nexus.cluster.workshops.gru.example-domain.com	XX.XX.81.82
vault.cluster.workshops.gru.example-domain.com	XX.XX.81.82
mattermost.cluster.workshops.gru.example-domain.com	XX.XX.81.82
awx.cluster.workshops.gru.example-domain.com	XX.XX.81.82
app10.dev.workshops.gru.example-domain.com	XX.XX.81.82
s10.dev.workshops.gru.example-domain.com	XX.XX.81.82
app1.dev.workshops.gru.example-domain.com	XX.XX.81.82
s1.dev.workshops.gru.example-domain.com	XX.XX.81.82
app2.dev.workshops.gru.example-domain.com	XX.XX.81.82
s2.dev.workshops.gru.example-domain.com	XX.XX.81.82
app3.dev.workshops.gru.example-domain.com	XX.XX.81.82
s3.dev.workshops.gru.example-domain.com	XX.XX.81.82
app4.dev.workshops.gru.example-domain.com	XX.XX.81.82
s4.dev.workshops.gru.example-domain.com	XX.XX.81.82
app5.dev.workshops.gru.example-domain.com	XX.XX.81.82
s5.dev.workshops.gru.example-domain.com	XX.XX.81.82
app6.dev.workshops.gru.example-domain.com	XX.XX.81.82
s6.dev.workshops.gru.example-domain.com	XX.XX.81.82
app7.dev.workshops.gru.example-domain.com	XX.XX.81.82
s7.dev.workshops.gru.example-domain.com	XX.XX.81.82
app8.dev.workshops.gru.example-domain.com	XX.XX.81.82
s8.dev.workshops.gru.example-domain.com	XX.XX.81.82
app9.dev.workshops.gru.example-domain.com	XX.XX.81.82
s9.dev.workshops.gru.example-domain.com	XX.XX.81.82
showcase.dev.workshops.gru.example-domain.com	XX.XX.81.82
api.dev.workshops.gru.example-domain.com	XX.XX.81.82
admin.dev.workshops.gru.example-domain.com	XX.XX.81.82
vault.dev.workshops.gru.example-domain.com	XX.XX.81.82
pgnav.example-domain.com	XX.XX.81.82

DMARC Check

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism for policy distribution by which an organization that is the originator of an email ensures that it is protected from phishing, spoofing or fraud attacks. It ensures that legitimate emails are properly authenticated and fraudulent activity which appear to come a domain under the organisation control is blocked before reaching end customer.

```
v=DMARC1; p=none; rua=mailto:DMARC@example-domain.com
```

Tag	Name	Description	Tag Value
v	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.	DMARC1
p	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.	none
rua	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.	mailto:DMARC@example-domain.com

Tests	Result
Dmarc Validity	Valid
DMARC Policy	Enabled
DMARC Syntax	The record is valid

A DMARC policy allows a sender's domain to indicate that their emails are protected by SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes - such as to reject the message or quarantine it. The policy can also specify how an email receiver can report back to the sender's domain about messages that pass and/or fail.

Geolocation Information

Eyesight determines the geolocation of the IP addresses asssociated to the organisation. Eyesight attempts to pinpoint which country an IP address is associated with using information from the RIRs (Regional Internal Registries) and other location data.

IP Address	Geolocation
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000

XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000
XX.XX.81.88	redacted, WWW, ZipCode-00000

Management Access Advisory From Aruba

In the past few years, there has been an increased focus across the security industry on the risks of exposing internal services to the public Internet. The explosion of the Internet-of-Things trend, with the addition of (frequently insecure) web interfaces to small devices in corporate and home networks, has helped push the risks that exposing internal network services to the Internet can pose into the general consciousness.

Eyesight leverages Shodan search engine to expose insecure Aruba server instances across the Internet. This module guides administrators through the process of limiting access to the management interfaces of the Aruba Access Point, Aruba Controller and Aruba ClearPass products.

This is not an Aruba instance.

Cisco Umbrella Risk Score

The Umbrella Investigate Risk Score is based on an analysis of the lexical characteristics of the domain name and patterns in queries and requests to the domain. It is scaled from 0 to 100, with 100 being the highest risk and 0 being no risk at all. Periodically Umbrella updates this score based on additional inputs. A domain blocked by Umbrella receives a score of 100.

The Cisco Umbrella has classified this domain to be Low Risk.

Malicious Domain Check

Cisco Umbrella keeps a database of all websites that have been known to be malicious and prevents users from accessing the site. The results from the subdomain discovery were further verified against Cisco Umbrella database to identify these malicious domains.

No malicious domains were identified associated with the domain provided.

The Umbrella Investigate integration with Cisco AMP Threat Grid shows samples from the ThreatGrid database associated with a domain, IP or URL that you're looking to find out more information about. Information about samples is provided in the form of checksums associated when looking up a specific host or IP.

Eyesight was not able to identify any malware samples associated with the domain.

Open Network Ports

Publicly accessible ports increase organisation's security risk especially when these belong to sensitive application on the server. The following section identifies all the open ports/services accessible publicly.

IP Address XX.XX.236.11

Port	Version or Response
443	443 HTTP/1.0 503 Service Unavailable Cache-Control: no-cache Connection: cl..

IP Address XX.XX.81.71

Port	Version or Response
443	443 Microsoft IIS httpd 8.5..

IP Address XX.XX.0.32

Port	Version or Response

80	80 HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content..

IP Address XX.XX.20.134

Port	Version or Response
4443	4443 Apache httpd..
443	443 Apache httpd..

IP Address XX.XX.221.162

Port	Version or Response
443	443 SSL Error: TLSV1_UNRECOGNIZED_NAME..
80	80 Apache httpd..

IP Address XX.XX.81.74

Port	Version or Response
443	443 Microsoft IIS httpd 8.5..

IP Address XX.XX.161.184

Port	Version or Response
80	80 HTTP/1.1 200 OK Date: Tue, 11 May 2021 03:31:26 GMT Content-Type: text/h..
995	995 +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CO..
587	587 550 Your host is not allowed to connect to this server...
21	21 Pure-FTPd..
25	25 550 Your host is not allowed to connect to this server...
443	443 cpe:/a:php:php cpe:/a:mysql:mysql cpe:/a:wordpress:wordpress cpe:/a:wor..
993	993 * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMES..
3306	3306 MySQL 5.5.5-10.3.28-MariaDB..
465	465 Exim smtpd 4.94..
2082	2082 HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="ut..

IP Address XX.XX.5.9

Port	Version or Response
443	443 HTTP/1.1 302 302 Date: Mon, 10 May 2021 22:32:06 GMT Expires: Thu, 01 J..
80	80 Apache httpd..

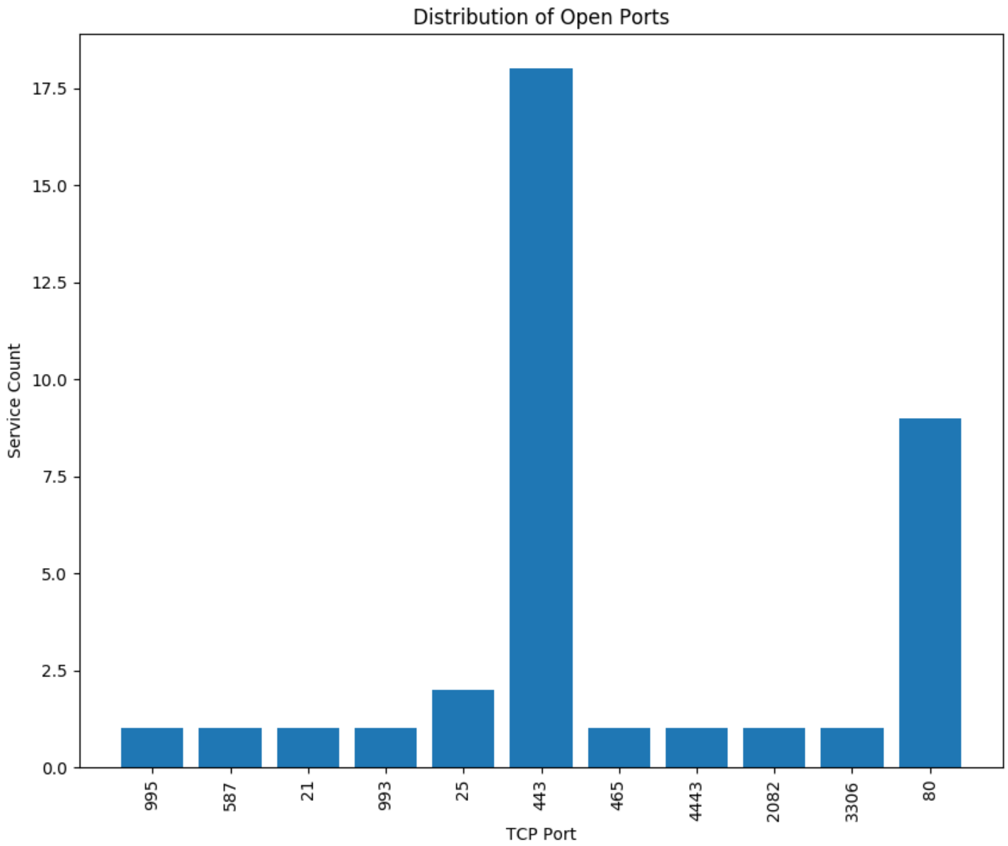
IP Address XX.XX.125.207

Port	Version or Response
443	443 HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Conten..

Sensitive Ports (Exposed)

The open ports can be dangerous when the service listening on the port is misconfigured, unpatched, vulnerable to exploits, or has poorly configured security rules. The following section describes the security risks produces by some of the above disclosed open TCP ports.

The following graph demonstrates the open TCP ports across the target domain and its subdomains:



The detailed list of publicly accessible services in the domain is below:

MySQL Protocol	PORT: 3306
Risk	Allowing remote access to MySQL is not a vulnerability by itself, but in certain events such as leaking of the database configuration file (contains credentials), an attacker will gain access to the MySQL server publicly.
Recommendation	Avoid using the default port for database service and ensure that service traffic is monitored by the

	firewall. Furthermore, implement IP based access restrictions.

FTP (File Transfer Protocol)	PORT: 21
Risk	FTP is often considered as an insecure protocol as data is sent in clear text format and offers an anonymous option with no password request.
Recommendation	Ensure that access to the service is password protected and anonymous login is disabled. Furthermore, enforce IP white-list on the service thereby allowing only limited access to the port.

SMTP (Simple Mail Transfer Protocol)	PORT: 25
Risk	If the service is not monitored or configured, spammers can connect to the target server and send unsolicited emails.
Recommendation	Specify trusted sources which can connect into your network on this Port using a firewall or the mail server. On an Exchange server, this can be achieved by creating a Receive Connector and only allowing it to accept SMTP traffic from designated IP's.

Finding 4: Each exposed port to the public internet is a front door for the attacker to try and infiltrate. During reconnaissance certain services were identified that were publicly accessible which may be unused by the application. When legitimate services are exposed to public internet, these may be exploited through code execution or miss-configurations.

[Severity of this risk: LOW]

Vulnerable Services

The open ports discovered from the previous sections are analysed for vulnerabilities using IOT search engine "Shodan". It allows the security experts to easily locate poorly protected devices exposed over the internet. At the same time, it represents a privileged instrument for the hackers that have to search for a specific target and need to gather information on its configuration.

The following outdated software(s) were discovered:

- The software hosted on TCP port **4443** in host IP **XX.XX.20.134** is running an outdated software **Apache httpd**
- The software hosted on TCP port **443** in host IP **XX.XX.29.10** is running an outdated software **Microsoft IIS httpd 7.5**

Refer to "Appendix: CVE (Outdated Software)" section for more information on the impacting vulnerabilities.

Finding 5: There are technologies installed on the server which are outdated and are having vulnerabilities. If there are known exploits in exploit databases(or deep web) for these vulnerabilities, an attacker may leverage these and gain access to the organisation network.

[Severity of this risk: HIGH]

SSL/TLS Information

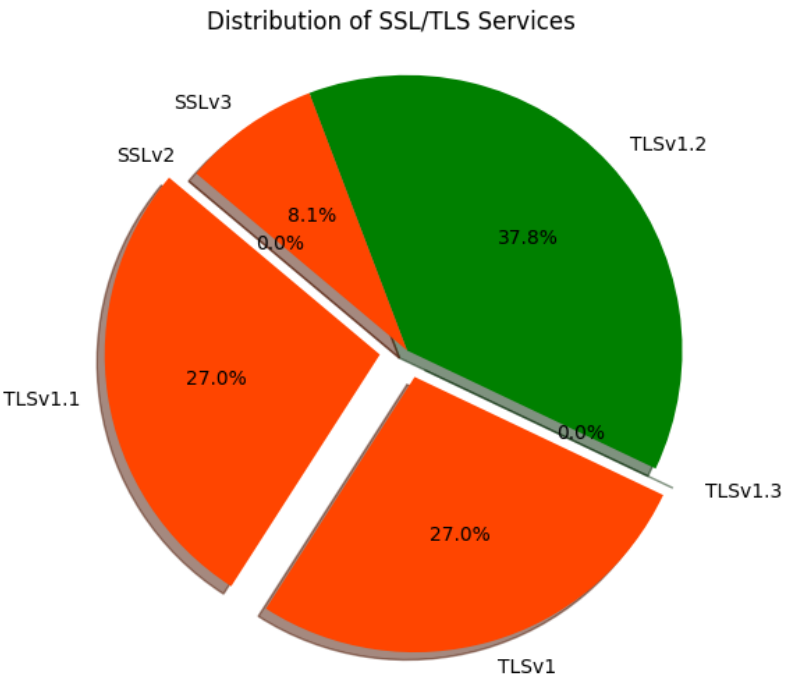
When a user connects to a web site with HTTPS, the application server returns a list of ciphers to encrypt the data stream. If weak ciphers were offered, secure communications can easily be defeated by a skilled attacker.

Furthermore, the SSL certificates are used to create an encrypted channel between the client and the server. They are means to offer trust to the end user and an assurance that they are communicating with the indented party.

The services employing SSL/TLS are investigated further and following information was gathered:

Service	443 (https) (XX.XX.236.11)
Accepted SSL/TLS Protocols	TLSv1 SSLv3 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.37.102)
Accepted SSL/TLS Protocols	TLSv1 SSLv3 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.175.116)
Accepted SSL/TLS Protocols	TLSv1 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.5.24)
Accepted SSL/TLS Protocols	TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.8.10)
Accepted SSL/TLS Protocols	TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.29.10)
Accepted SSL/TLS Protocols	TLSv1 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.5.29)
Accepted SSL/TLS Protocols	TLSv1 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.81.72)
Accepted SSL/TLS Protocols	TLSv1 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.173.117)
Accepted SSL/TLS Protocols	TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False
Service	443 (https) (XX.XX.81.89)
Accepted SSL/TLS Protocols	TLSv1 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha256WithRSAEncryption (Bits: 2048, Type: rsa)
Is Certificate Expired:	False

The following graph demonstrates the services using SSL/TLS protocols across the target domain and its subdomains:



Outdated SSL/TLS Protocols

On March of 2020, Firefox and other popular browsers disabled the support of TLS 1.1 along with TLS 1.0. As these protocols do not support modern cryptographic algorithms, their existence on the application server remains a security risk.

The employment of the latest TLS version such TLS1.2 and higher, come with many benefits:

- These have desirable performance and security properties, such as perfect forward secrecy and authenticated encryption.
- As part of peer authentication, mandatory and insecure SHA-1 and MD5 hash functions were removed.
- Resistance to downgrade-related attacks such as FREAK.

The following services use outdated SSL/TLS ciphers:

- TCP PORT: 443 (XX.XX.81.89)
- TCP PORT: 443 (XX.XX.81.89)
- TCP PORT: 443 (XX.XX.81.89)
- TCP PORT: 443 (XX.XX.81.89)
- TCP PORT: 443 (XX.XX.81.89)
- TCP PORT: 443 (XX.XX.81.89)
- TCP PORT: 443 (XX.XX.81.89)
- TCP PORT: 443 (XX.XX.81.89)

Finding 6: TLS scans identified the domain www.example-domain.com to use outdated cipher suites that are often vulnerable to attacks. These protocols may be affected by vulnerabilities such as FREAK, POODLE, BEAST, and CRIME. If supporting TLS 1.0 is a business requirement, disable TLS 1.0 compression to avoid CRIME attacks. *[Severity of this risk: LOW]*

Expired Security Certificates

Security Certificate expire after a certain validity period and this is means to provide assurance to the security of SSL. The validity period regulates and confirms the authenticity of the server to the web browsers. Among the gathered domain related hosts, the security certificate of the following services were found expired:

- TLS Certificate of the service hosted on TCP PORT 443 (XX.XX.236.11) has expired.
- TLS Certificate of the service hosted on TCP PORT 443 (XX.XX.81.68) has expired.

Finding 7: Certificate seems to have been expired on services of the domain www.example-domain.com. This puts the personal information of the customers at risk especially when sensitive operations such as financial transaction are carried out. This can also results in decline in sales and revenue as customers do not trust site any more. *[Severity of this risk: MEDIUM]*

Appendix: Additional Gathered intelligence

The following sections describes the various tests conducted on the domain(s).

DNS Lookup

Below are the DNS records for a domain determined using the dig DNS tool.

Record	Value
A	XX.XX.221.161
CNAME	srvweb3.example-domain.com.

WHOIS Lookup

WHOIS database provides information on domain registration and availability.

WHOIS Result

```
Domain Name: EXAMPLE-DOMAIN.COM
   Registry Domain ID: 382015_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.gandi.net
   Registrar URL: http://www.gandi.net
   Updated Date: 2021-02-01T10:53:17Z
   Creation Date: 1997-03-07T05:00:00Z
   Registry Expiry Date: 2022-03-08T05:00:00Z
   Registrar: Gandi SAS
   Registrar IANA ID: 81
   Registrar Abuse Contact Email: abuse@support.gandi.net
   Registrar Abuse Contact Phone: +33.170377661
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: A.DNS.GANDI.NET
   Name Server: B.DNS.GANDI.NET
   Name Server: C.DNS.GANDI.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-05-11T13:31:26Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
```

```
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: example-domain.com
Registry Domain ID: 382015_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2021-02-01T11:53:17Z
Creation Date: 1997-03-07T00:00:00Z
Registrar Registration Expiration Date: 2022-03-08T05:00:00Z
Registrar: GANDI SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller: EXAMPLE-DOMAIN
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: BERGER LEVRAULT
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: FR
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: d3f9c3feb70942b104f9df41df03372c-755772@contact.gandi.net
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
```

```
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext:
Admin Email: d3f9c3feb70942b104f9df41df03372c-755772@contact.gandi.net
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext:
Tech Email: d3f9c3feb70942b104f9df41df03372c-755772@contact.gandi.net
Name Server: A.DNS.GANDI.NET
Name Server: B.DNS.GANDI.NET
Name Server: C.DNS.GANDI.NET
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-05-11T13:31:45Z <<<

For more information on Whois status codes, please visit
https://www.icann.org/epp

Reseller Email:
Reseller URL:

Personal data access and use are governed by French law, any use for the purpose of unsolicited mass
commercial advertising as well as any mass or automated inquiries (for any intent other than the
registration or modification of a domain name) are strictly forbidden. Copy of whole or part of our
database without Gandi's endorsement is strictly forbidden.
A dispute over the ownership of a domain name may be subject to the alternate procedure established
by the Registry in question or brought before the courts.
For additional information, please contact us via the following form:
 https://www.gandi.net/support/contacter/mail/
```

Domain Subnets

The section lists the subnet ranges of the organisation(s) from public sources like ipv4list.info and several others.

```
IP Info
Address      = XX.XX.221.161
Network      = XX.XX.221.161 / 32
Netmask      = 255.255.255.255
Broadcast    = not needed on Point-to-Point links
Wildcard Mask = 0.0.0.0
```

```
Hosts Bits    = 0
Max. Hosts    = 1   (2^0 - 0)
Host Range    = { XX.XX.221.161 - XX.XX.221.161 }
```

Reverse IP Lookup

Reverse IP lookup lets identifies the websites hosted on a server.

Domain List
example-domain.com
example-domain.fr
bl-citoyen.com
boutique.example-domain.com
cabinetnumerique.example-domain.com
cabinetnumeriqueaudit.example-domain.com
cabinetnumeriquetest.example-domain.com

If there is a security breach on any of the hosted websites, all other websites sharing this host may also be impacted. This setup does not offer any protection even if these websites are running the latest software and protected by WAF.

[Severity : Remark]

Appendix: Known Breaches

Breach Name	Description
db8151dd	In February 2020, a massive trove of personal information referred to as db8151dd was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.
Apollo	In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their revenue acceleration platform and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.
Cit0day	In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.
2844Breaches	In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single unverified data breach.
Nitro	In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.

Appendix: CVE (Outdated Software)

The vulnerabilities impacting the software Apache httpd on TCP port (4443)(XX.XX.20.134)

Note that the host/device may not be impacted by all of these issues mentioned below. The vulnerabilities are implied based on the software and version.

CVE	CVSS	Verified	Summary
CVE-2018-10549	6.8	False	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
CVE-2018-10548	5.0	False	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
CVE-2018-10545	1.9	False	An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.
CVE-2018-10547	4.3	False	An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.
CVE-2018-10546	5.0	False	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.
CVE-2019-9641	7.5	False	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

CVE-2018-19520	6.5	False	An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.
CVE-2018-19396	5.0	False	ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.
CVE-2018-19395	5.0	False	ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").
CVE-2018-19935	5.0	False	ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.
CVE-2018-17082	4.3	False	The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.
CVE-2019-9639	5.0	False	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.
CVE-2019-9638	5.0	False	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.
CVE-2019-9637	5.0	False	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly

			available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.
CVE-2018-14883	5.0	False	An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.
CVE-2018-20783	5.0	False	In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.
CVE-2019-6977	6.8	False	gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.
CVE-2013-6420	7.5	False	The asn1_time_to_time_t function in ext/openssl/openssl.c in PHP before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7 does not properly parse (1) notBefore and (2) notAfter timestamps in X.509 certificates, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate that is not properly handled by the openssl_x509_parse function.
CVE-2019-9023	7.5	False	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.

CVE-2019-9020	7.5	False	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.
CVE-2019-9021	7.5	False	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.
CVE-2017-16642	5.0	False	In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.
CVE-2019-9024	5.0	False	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.
CVE-2018-15132	5.0	False	An issue was discovered in ext/standard/link_win32.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. The linkinfo function on Windows doesn't implement the open_basedir check. This could be abused to find files on paths outside of the allowed directories.

The vulnerabilities impacting the software Microsoft IIS httpd 7.5 on TCP port (443)(XX.XX.29.10)

Note that the host/device may not be impacted by all of these issues mentioned below. The vulnerabilities are implied based on the software and version.

CVE	CVSS	Verified	Summary
CVE-2010-1899	4.3	False	Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."
CVE-2010-2730	9.3	False	Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."
CVE-2010-3972	10.0	False	Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.
CVE-2012-2531	2.1	False	Microsoft Internet Information Services (IIS) 7.5 uses weak permissions for the Operational log, which allows local users to discover credentials by reading this file, aka "Password Disclosure Vulnerability."
CVE-2012-2532	5.0	False	Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) processes unspecified commands before TLS is enabled for a session, which allows remote attackers to obtain sensitive information by reading the replies to these commands, aka "FTP Command Injection Vulnerability."
CVE-2010-1256	8.5	False	Unspecified vulnerability in Microsoft IIS 6.0, 7.0, and 7.5, when Extended Protection for Authentication is enabled, allows remote authenticated users to execute arbitrary code via unknown vectors related to "token checking" that trigger memory corruption, aka "IIS Authentication Memory Corruption Vulnerability."

INGRAM MICRO
SECURITY

NETFORMERS
Engineering Your Future

INGRAM MICRO

ISSY LES MOULINEAUX

GREATER PARIS REGION

FR

Ingram Micro B.V - Papendorpseweg 95 - 3528 BJ Utrecht – The Netherlands
NetFormers - ul. Czeska 24/2, 03-902 Warszawa