

Attack Surface Report

[Redacted]

Dec 12, 2022

About This Report

An Attack Surface is the number of points, or attack vectors, across your IT network where unauthorized users could exploit vulnerabilities to gain access to systems, extract confidential data, and stage an attack.

As new technologies, services, and connections are introduced, your Attack Surface expands, increasing the number of attack vectors and the overall risk for your business. By taking the time to understand, measure, and reduce your attack surface, you can improve your cyber security posture and prevent attacks.














This report leverages open-source data to measure your External Attack Surface, including possible attack vectors externally accessible to the internet. You can complement this report by increasing your situational awareness across your entire IT network, including endpoints, network, and cloud environments.

About SFY

SFY Information Technology utilizes industry leading security tools to bringing advanced cyber security solutions and services to businesses of all sizes. After years of research and development by the brightest in the business, we have pioneered a holistic approach to cyber security.

Our complete Managed Detection and Response (MDR) solution, flexible simulation-based training platform, and expert-led professional services form a unified defence that results in superior security, less complexity, and immediate value. We build solutions that are sophisticated, yet easy to use and manage, so every business owner can get the hands-free cyber security they expect. For more information, visit sfy.ca.

Table of Contents

-  **Executive Summary**3
-  1. End of Life (EOL) Software4
-  2. End of Life (EOL) Operating Systems5
-  3. Potentially Vulnerable Systems6
-  4. Remote Access7
-  5. Email (SPF and DMARC)8
-  6. Industrial Control Systems (ICS)9
-  7. Internet of Things (IOT)10
-  8. Insecure Protocols11
-  9. Transport Layer Security (TLS)12
-  10. Certificates13
-  11. Databases14
-  12. Other Issues15
- About the Data Source16
- Full Logs (Annex A)17

Executive Summary

Overall Risk: High



A high number of security issues were noted in the automated analysis of your organization's Internet-facing IP Addresses.

The following actions are recommended:

1. Review the full details of the report.
2. Develop a plan (including necessary resources) to remediate the most serious issues.
3. Consider installing a holistic cyber security monitoring product such as Covalence on your organization's network, to increase visibility of your entire attack surface and stop cyber threats.

1. End of Life (EOL) Software

An EOL product is a software application which is at the end of its product lifecycle and is no longer receiving updates, including security updates. EOL products are particularly vulnerable to hacking as they often have publicly known exploits for which there is no patch.

Analysis Results



- The following EOL software products were found in your organization's Internet-facing IP space:
 - Lotus Domino httpd
 - Microsoft IIS httpd 6.0
 - PHP Version 7.3.29

It is recommended that these applications be upgraded as soon as possible.

2. End of Life (EOL) Operating Systems

An EOL operating system is at the end of its product lifecycle and is no longer receiving updates, including security updates. EOL operating systems are particularly vulnerable to hacking as they often have publicly known exploits for which there is no patch.

Analysis Results



- No Internet-facing EOL operating systems were noted during the analysis.

3. Potential Vulnerabilities

Hackers and security researchers are constantly looking for new vulnerabilities in computer systems and software. When new vulnerabilities are disclosed publicly they are given a designator under the Common Vulnerabilities and Exposures (CVE) system to track them.

Analysis Results



- A total of 96 known vulnerabilities (CVEs) for 9 IP(s) were noted on your Internet-facing infrastructure. See Annex A for more details.

These IPs warrant special attention for patching and MDR protection.

4. Remote Access

Remote Access includes protocols like RDP, VNC, and TeamViewer that allow remote administration of computers. It could also include the administration interface of an important network device like a firewall or router.

Analysis Results



- No Remote Administration issues were noted during the analysis.

5. Email (SPF and DMARC)

SPF (Sender Policy Framework) and DMARC (Domain-based Message Authentication, Reporting and Conformance) are security configurations that are added to servers to increase the security of email.

SPF and DMARC help protect your domain against spoofing and decrease the chances that messages originating from your organization will be marked as spam.

Analysis Results



- DMARC record found for domain: [REDACTED]
- SPF record found for domain: [REDACTED]

6. Industrial Control Systems (ICS)

ICS devices are used for industrial processes or building automation. They should never be positioned to allow inbound connections from the Internet because they typically have no or weak authentication and were not designed with security as a top priority.

Analysis Results



-
- No ICS systems were noted during the analysis.

7. Internet of Things (IOT)

IOT devices such as smart lightbulbs and door locks should never allow inbound connections from the Internet due to their simple design and lack of security. IOT devices provide an excellent entry point for threat actors, who can then move laterally to internal IP addresses.

In 2018 hackers were able to steal customer data from a casino database server by first gaining access to their network via an internet-connected aquarium thermometer ([Link](#)).

Analysis Results



- No IOT systems were noted during the analysis.

8. Insecure Protocols

Older Internet protocols such as FTP and POP3 are plaintext and typically only protected with a single factor of authentication (password). Their use should be limited and reviewed frequently with the goal of complete removal.

If your organization is still running insecure websites on TCP/80 (HTTP) we recommend moving to TLS (HTTPS) only.

Analysis Results



- The following insecure protocols are likely in use on your network:

- FTP (TCP/21)
- HTTP (TCP/10001)
- HTTP (TCP/6080)
- HTTP (TCP/80)
- IMAP (TCP/143)
- POP3 (TCP/110)

See Annex A for more details.

9. Transports Layer Security (TLS)

Transport Layer Security (TLS) is a critical security protocol used to protect web traffic. It provides confidentiality and integrity of data in transit between clients and servers exchanging information.

Several encryption standards in the TLS/SSL families have been deprecated since 2011. The driving force behind the deprecation process was the large number of attacks which impacted the cryptographic algorithms at the base of the two protocols. This included attacks such as BEAST, POODLE, and LUCKY 13, all of which showed how attackers could take advantage of weaknesses in both SSL and TLS 1.0/1.1 to compromise encrypted communications and attack organizations.

Analysis Results



- The following deprecated encryption protocols were noted during the analysis:

- TLSv1
- SSLv3
- TLSv1.1

It is recommended that the necessity of having these protocols available be assessed. See Annex A for more details.

10. Certificates

SSL Certificates are files used to establish secure communications channels between servers and visitors (clients). Without certificate-based encryption, Internet traffic is vulnerable to eavesdropping and man-in-the-middle attacks.

Expired certificates, the use of wildcard certificates, and self-signed certificates can increase your organization's level of risk and impact your reputation.

Analysis Results



- The following certificate issues were noted during the analysis:
 - Expired Certificates
 - Expiring Certificates (next 2 months)
 - Self-signed Certificates

See Annex A for more details.

11. Databases

Organizations should be wary of directly connecting database servers to the Internet, as they typically lack multifactor authentication and present an enticing target to cybercriminals. These criminals are increasingly stealing the records from databases to extort their victims into large payments.

Analysis Results



- No database servers were noted during the analysis.

12. Other Issues

Other security issues were noted on your network during the automated analysis. These issues may impact the privacy of your organization or increase the chances that an attacker can gain control of one of your Internet-facing devices.

Analysis Results



- The following additional issues were noted:
 - Email server without STARTTLS enabled

Additional Observations

No observations to report.

About the Data Source

The data for this report was retrieved from Shodan (www.shodan.io), and other publicly available sources. The Shodan service regularly scans the entire Internet on well-known ports looking for connected devices. It is used extensively by security researchers like those at Field Effect but has been dubbed “The World’s Most Dangerous Search Engine” because it is also heavily leveraged by hackers to find exploitable networks.

At no point during this analysis were any penetration testing activities directed at your organization’s networks. All the data contained in this report is publicly available to both security researchers and hackers alike.

Annex A: Full Output Logs

Section 1- Found EOL device: Lotus Domino httpd at IP: [REDACTED]
Section 1- Found EOL device: Lotus Domino httpd at IP: [REDACTED]
Section 1- Found EOL device: Lotus Domino httpd at IP: [REDACTED]
Section 1- Found EOL product: PHP Version 7.3.29 at IP: [REDACTED]
Section 1- Found EOL service: Microsoft IIS httpd Version:6.0 at IP: [REDACTED]
Section 3- 1 potential CVEs noted for IP: [REDACTED]
Section 3- 1 potential CVEs noted for IP: [REDACTED]
Section 3- 1 potential CVEs noted for IP: [REDACTED]
Section 3- 1 potential CVEs noted for IP: [REDACTED]
Section 3- 1 potential CVEs noted for IP: [REDACTED]
Section 3- 1 potential CVEs noted for IP: [REDACTED]
Section 3- 2 potential CVEs noted for IP: [REDACTED]
Section 3- 5 potential CVEs noted for IP: [REDACTED]
Section 3- 88 potential CVEs noted for IP: [REDACTED]
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 80
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 80
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 80
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 80
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 80
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 80
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 6080
Section 8- Found deprecated protocol (HTTP) running on IP: [REDACTED] Port: 80
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 21
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 143
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 21
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 110
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 21
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 143
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 110
Section 8- Found deprecated protocol running on IP: [REDACTED] Port: 143
Section 9- Found deprecated TLS protocol SSLv3 at IP: [REDACTED]
Section 9- Found deprecated TLS protocol TLSv1 at IP: [REDACTED]
Section 9- Found deprecated TLS protocol TLSv1 at IP: [REDACTED]
Section 9- Found deprecated TLS protocol TLSv1 at IP: [REDACTED]
Section 9- Found deprecated TLS protocol TLSv1.1 at IP: [REDACTED]
Section 9- Found deprecated TLS protocol TLSv1.1 at IP: [REDACTED]
Section 10- Certificate at IP: [REDACTED]:443 expiring: 2023-01-13 19:36:30
Section 10- Certificate at IP: [REDACTED]:443 expiring: 2023-01-04 00:50:51
Section 10- Expired certificate found at IP: [REDACTED]:443
Section 10- Expired certificate found at IP: [REDACTED]:443



Section 10- Expired certificate found at IP: [REDACTED]:443
Section 10- Expired certificate found at IP: [REDACTED]:443
Section 10- Expired certificate found at IP: [REDACTED]:443
Section 10- Expired certificate found at IP: [REDACTED]:443
Section 10- Self-signed certificate found at IP: [REDACTED]
Section 10- Self-signed certificate found at IP: [REDACTED]
Section 10- Self-signed certificate found at IP: [REDACTED]
Section 12- Email server without STARTTLS enabled found at IP: [REDACTED] Port: 25
Section 12- Email server without STARTTLS enabled found at IP: [REDACTED] Port: 25
Section 12- Email server without STARTTLS enabled found at IP: [REDACTED] Port: 25