MyRepublic™

ATTACK SURFACE MANAGEMENT REPORT

Prepared for: myrepublicapp.com

Date: 2025-06-04

TABLE OF CONTENTS

1. Assessment Summary

MyRepublic performed an "Attack Surface Assessment" against **myrepublicapp.com** 's internet-facing assets. Cyber attackers targeting your organization will start by "looking from the outside in". This assessment report imitates this perspective of your organization's external surface, including potential entry points and their weaknesses or vulnerabilities.

The scan uses advanced tools and techniques to uncover details from your network and web layers, as well as relevant public information. The findings in this report could also be or might already have been discovered by actual attackers over the public Internet.

The domain name **myrepublicapp.com** was used as the starting point of this scan.

Subdomains	Endpoints	Vulnerabilities
16	22	38

Vulnerability Summary

VULNERABILITY CATEGORY	SUB-CATEGORY	RISK	COUNT
System security	Jenkins Git <=4.11.3 - Missing Authorization	HIGH	1
System security	OpenSSH Terrapin Attack - Detection	MEDIUM	10
System security	Weak Cipher Suites Detection	LOW	18
System security	Mismatched SSL Certificate	LOW	6
System security	SSH Server CBC Mode Ciphers Enabled	LOW	1
System security	SSH Weak Key Exchange Algorithms Enabled	LOW	1
System security	SSH Diffie-Hellman Modulus <= 1024 Bits	LOW	1

2. Findings

Each security finding in this report has a category and subcategory and includes the affected asset, details of the finding and the associated risk. The risk score considers both the impact of the finding and how easy it is for an attacker to actually exploit it.

2.1 System Security

Each of your Internet-facing hosts identified during MyRepublic's scan is running an operating system with some software and services. Attackers will inspect any system services and software that is exposed to the Internet to find security issues on your attack surface.

2.2 Known Software Vulnerabilities

When critical zero-day vulnerabilities are publicly released, the software provider will release a patch to fix the issue, but the asset would only be considered secured after the version is upgraded. These software vulnerabilities become public knowledge, usually in the Common Vulnerabilities and Exposures (CVE) database.

Jenkins Git <=4.11.3 - Missing Authorization

HIGH

CVSS SCORE

```
7.5
```

DESCRIPTION

Jenkins Git plugin through 4.11.3 contains a missing authorization check. An attacker can trigger builds of jobs configured to use an attacker-specified Git repository and to cause them to check out an attacker-specified commit. This can make it possible to obtain sensitive information, modify data, and/or execute unauthorized operations.

AFFECTED ASSET

https://jenkins.dst.myrepublicapp.com/git/notifyCommit?url=2y1oe6jrW5pZDyEALnayWgD76QS&branches=2y1oe6jrW5pZDyEALnayWgD76QS

REFERENCES

- https://www.jenkins.io/security/advisory/2022-07-27/#SECURITY-284
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-36883
- https://nvd.nist.gov/vuln/detail/CVE-2022-36883
- http://www.openwall.com/lists/oss-security/2022/07/27/1
- https://github.com/StarCrossPortal/scalpel

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet

Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://ux.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://ux3.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://ux4.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://ux5.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://boss.dst.myrepublicapp.com:22

REFERENCES

- https://github.com/RUB-NDS/Terrapin-Scanner
- https://terrapin-attack.com/

- http://packetstormsecurity.com/files/176280/Terrapin-SSH-Connection-Weakening.html
- http://seclists.org/fulldisclosure/2024/Mar/21
- http://www.openwall.com/lists/oss-security/2023/12/18/3

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://jenkins.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://ux0.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense

CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://api-ext.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://ux1.dst.myrepublicapp.com:22

OpenSSH Terrapin Attack - Detection

MEDIUM

CVSS SCORE

```
5.9
```

DESCRIPTION

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

AFFECTED ASSET

http://order.dst.myrepublicapp.com:22

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux3.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux4.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux0.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux4.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://order.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://order.dst.myrepublicapp.com

SSH Diffie-Hellman Modulus <= 1024 Bits

LOW

DESCRIPTION

SSH weak algorithms are outdated cryptographic methods that pose security risks. Identifying and disabling these vulnerable algorithms is crucial for enhancing the overall security of SSH connections.

AFFECTED ASSET

http://jenkins.dst.myrepublicapp.com:22

REFERENCES

- https://access.redhat.com/solutions/4278651

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux5.dst.myrepublicapp.com

Mismatched SSL Certificate

LOW

DESCRIPTION

Mismatched certificates occur when there is inconsistency between the common name to which the certificate was issued and the domain name in the URL. This issue impacts the trust value of the affected website.

AFFECTED ASSET

https://ux1.dst.myrepublicapp.com

REFERENCES

- https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssl-certificate-name-hostname-mismatch/

Mismatched SSL Certificate

LOW

DESCRIPTION

Mismatched certificates occur when there is inconsistency between the common name to which the certificate was issued and the domain name in the URL. This issue impacts the trust value of the affected website.

AFFECTED ASSET

https://ux5.dst.myrepublicapp.com

Mismatched SSL Certificate

LOW

DESCRIPTION

Mismatched certificates occur when there is inconsistency between the common name to which the certificate was issued and the domain name in the URL. This issue impacts the trust value of the affected website.

AFFECTED ASSET

https://ux.dst.myrepublicapp.com

Mismatched SSL Certificate

LOW

DESCRIPTION

Mismatched certificates occur when there is inconsistency between the common name to which the certificate was issued and the domain name in the URL. This issue impacts the trust value of the affected website.

AFFECTED ASSET

https://ux0.dst.myrepublicapp.com

Mismatched SSL Certificate

LOW

DESCRIPTION

Mismatched certificates occur when there is inconsistency between the common name to which the certificate was issued and the domain name in the URL. This issue impacts the trust value of the affected website.

AFFECTED ASSET

https://ux4.dst.myrepublicapp.com

Mismatched SSL Certificate

LOW

DESCRIPTION

Mismatched certificates occur when there is inconsistency between the common name to which the certificate was issued and the domain name in the URL. This issue impacts the trust value of the affected website.

AFFECTED ASSET

https://ux3.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux5.dst.myrepublicapp.com

SSH Server CBC Mode Ciphers Enabled

LOW

DESCRIPTION

"SSH Server CBC Mode Ciphers Enabled" signifies that the SSH server supports Cipher Block Chaining (CBC) mode ciphers, which are known for potential vulnerabilities. This configuration poses a security risk, and it's recommended to disable CBC ciphers in favor of more secure alternatives for enhanced protection during data transmission.

AFFECTED ASSET

http://jenkins.dst.myrepublicapp.com:22

REFERENCES

- https://www.tenable.com/plugins/nessus/70658

SSH Weak Key Exchange Algorithms Enabled

LOW

DESCRIPTION

SSH Weak Key Exchange Algorithms Enabled indicates that the SSH server or client is configured to allow the use of less secure key exchange methods, posing a potential security risk during the establishment of secure connections. It's crucial to update configurations to prioritize stronger key exchange algorithms.

AFFECTED ASSET

http://jenkins.dst.myrepublicapp.com:22

REFERENCES

- https://www.tenable.com/plugins/nessus/153953

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux1.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://boss.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://api-ext.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux0.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux3.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://ux1.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://boss.dst.myrepublicapp.com

Weak Cipher Suites Detection

LOW

DESCRIPTION

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

AFFECTED ASSET

https://api-ext.dst.myrepublicapp.com

3. Discovered Assets and Subdomains

The following IP addresses and subdomains have been discovered for your organization:

SUBDOMAIN	IP ADDRESS	HTTP STATUS	VULNERABILITIES
order.dst.myrepublicapp.com	54.255.5.174	200	3
boss-newux.dst.myrepublicapp.com	54.251.215.35	200	0
boss.dst.myrepublicapp.com	3.1.242.55	200	3
jenkins.dst.myrepublicapp.com	18.140.251.57	403	5
ux5.dst.myrepublicapp.com	3.1.242.55	404	4
api-ext.dst.myrepublicapp.com	3.1.242.55	404	3
ux.dst.myrepublicapp.com	3.1.242.55	404	4
ux0.dst.myrepublicapp.com	3.1.242.55	404	4
ux1.dst.myrepublicapp.com	3.1.242.55	404	4
ux3.dst.myrepublicapp.com	3.1.242.55	404	4
ux4.dst.myrepublicapp.com	3.1.242.55	404	4
emr.myrepublicapp.com			0
myaccount.dst.myrepublicapp.com			0

SUBDOMAIN	IP ADDRESS	HTTP STATUS	VULNERABILITIES
dst.myrepublicapp.com			0
myrepublicapp.com			0
ux2.dst.myrepublicapp.com			0

NOTE: The asset discovery process by reNgine may not be exhaustive. It is possible that some of your assets may not be found by the current scan but may still be part of your attack surface.

4. Assessment Methodology

MyRepublic has developed a comprehensive system to assess an organization's attack surface. The assessments are automated and are based on how real attackers would approach an organization via the Internet.

This assessment should not be considered a full penetration test. Instead, it is modeled as an initial evaluation attackers would use to estimate how easy or difficult it would be to attack an organization from the external systems and services.

The following actions are performed by our assessments:

- Target identification and enumeration
- OSINT scanning
- Port scanning
- Network vulnerability scanning
- Web vulnerability scanning
- CVE database correlation
- Attack surface mapping

5. Report Disclaimer

Important Notice

This report is based on the information available at the time of the assessment and is limited to the systems and networks reviewed. The report assessment is not exhaustive and may not identify all vulnerabilities or risks. Any omissions or inaccuracies in the information provided may affect the findings and recommendations.

The report assessment should not be used for diagnosis, nor should it be considered a replacement for consultation and assessment with relevant cybersecurity professionals.

We do further note that while our recommendations may help you implement better cybersecurity practices, no system can be considered entirely secure. New vulnerabilities may arise in the future, and it is essential to maintain ongoing security efforts.

END OF REPORT