

 BRIEF

Vulnerabilities in TLS Communications

ZEROFOX INTELLIGENCE

B-2022-05-16a

Classification: White

Criticality: High

Intelligence Requirements: Vulnerability

May 16, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on May 16, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Vulnerabilities in TLS Communications

Executive Summary

Transport Layer Security (TLS) 1.0 and 1.1 have been strongly recommended for deprecation in order to adhere to new industry standards, mitigate risks of cyberattacks, and minimize the risk of misconfigurations. Recent developments, dubbed “TLStorm 2.0,” involved several critical vulnerabilities in TLS communications in multiple models of network switches, emphasizing the urgency of updating from outdated TLS versions to more secure versions. Most notably, these vulnerabilities include the possibility of hackers intercepting and decrypting traffic between a user's browser and an SSL-secured website.

Details

Transport Layer Security (TLS) 1.0 and 1.1 have been strongly recommended for deprecation in order to adhere to new industry standards, mitigate risks of cyberattacks, and minimize the risk of misconfigurations. TLS 1.0 and 1.1 are security protocols used to establish encryption channels across computer networks that have existed since 1999 and 2006, respectively. TLS 1.0 and 1.1 were both broadly deprecated by major websites around 2020. In March 2021, the Internet Engineering Task Force officially deprecated these protocols, and many organizations followed suit throughout the last year. For example, Payment Card Industry (PCI) standards require websites to stop supporting TLS 1.0 to remain PCI compliant.¹ All federal agencies were required to deprecate the use of TLS 1.0 and 1.1 due to security concerns - largely in 2020. Additionally, The National Institute of Standards and Technology began strongly recommending the use of more secure TLS versions in 2020.

Over the last month, critical vulnerabilities have been identified that impact multiple models of network switches. The vulnerabilities include five remote code execution (RCE) vulnerabilities that could result in the exfiltration of network traffic or sensitive

¹ <https://www.ssl.com/guide/tls-standards-compliance/>



information, as well as breakage of network segmentation and lateral movement to additional devices.² These vulnerabilities in turn impact multiple industries, notably the travel and healthcare industries, which heavily utilize the affected network switches. The vendors affected by these vulnerabilities are Aruba Networks (acquired by HPE) and Avaya Networking (acquired by ExtremeNetworks).³ In referencing these recent five RCE vulnerabilities, Aruba Networks indicated that “exploitation of these vulnerabilities would most likely occur as part of an attack chain building upon previous exploitation of customer-controlled infrastructure.”⁴

Analyst Commentary

NSA Issues Notice

In June 2017, the National Security Agency (NSA) issued a risk notice advising against the use of insecure TLS protocols. According to the notice, cryptographic exploits could be conducted passively from network locations that may not be monitored - or conducted - so that no indication of the exploit could be observed. This allows an adversary to go undetected and have continued access to sensitive data.

ROBOT Attack

In December 2017, security researchers at Ruhr-Universität Bochum/Hackmanit and Tripwire VERT discovered the return of a 19-year-old vulnerability in TLS dubbed “ROBOT.”⁵ It allowed for performing RSA decryption and signing operations with the private key of a TLS server; by using slight variations, the vulnerability could still have been used against many HTTPS hosts at the time. The flaw in RSA PKCS #1 v1.5 encryption was found to have affected the servers of 27 of the top 100 web domains, including Facebook and PayPal. It could have been exploited by an attacker to decrypt encrypted communications and steal sensitive and confidential data, including passwords, credit card data, and other sensitive details.⁶ According to the researchers, as long as compatibility with RSA encryption cipher suites was kept on older TLS versions, the attacks remained prevalent.

NIST Guidelines

In August 2019, The National Institute of Standards and Technology (NIST) published a revision to its “Guidelines for the Selection, Configuration, and Use of Transport

²

<https://portswigger.net/daily-swig/tlstorm-2-0-millions-of-aruba-and-avaya-network-switches-affected-by-rce-flaws>

³

<https://www.itsecurityguru.org/2022/05/03/tlstorm-2-0-airports-hospitals-hotels-and-enterprises-at-risk-to-new-vulnerabilities/>

⁴ <https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-008.txt>

⁵ <https://securityaffairs.co/wordpress/66682/hacking/robot-attack.html>

⁶ <https://www.robotattack.org/>



Layer Security (TLS) Implementations.” In the revised document, NIST stated that services using TLS 1.0 or 1.1 that access high-value data may increase the likelihood of a breach for relatively little gain in terms of accessibility.⁷ Two older types of attacks were referenced: the BEAST attack and the Klima attack. The BEAST attack (CVE-2011-3389) exploited issues with the TLS 1.0 implementation of Cipher Block Chaining (CBC) to decrypt parts of a packet, and specifically to decrypt HTTP cookies when HTTP is run over TLS. Also, the Klima attack, which relied on a version-check oracle, exploited alert messages sent during the SSL/TLS protocol resulting from incorrect lengths of the plaintext or from incorrect SSL/TLS version numbers contained in the plaintext.⁸ This gathered a small amount of information about the master key used for a previous SSL/TLS. According to cryptographer Klima, the leaked information could have been accumulated together so that the master key of a previous SSL/TLS session could be recovered, enabling the threat actor to decrypt all the messages protected during that session.⁹

IETF's Deprecation of TLS 1.0 and 1.1

In November 2020, the Internet Engineering Task Force (IETF) published a draft report on “Deprecating TLSv1.0 and TLSv1.1.” The report explained that these TLS versions lacked support for current and recommended cryptographic algorithms and mechanisms. Removing support for older TLS versions reduced the attack surface, lessened the opportunity for misconfiguration, and streamlined library and product maintenance. In March 2021, the IETF officially deprecated these protocols.

IETF's technical justification for the deprecation recommendation of TLS 1.0 and 1.1 is that:

- They require the implementation of older cipher suites that are no longer desirable for cryptographic reasons (e.g., TLSv1.0 makes TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA mandatory to implement).
- There is a lack of support for currently recommended cipher suites, especially AEAD ciphers that were not supported prior to TLSv1.2. (Note: registry entries for no-longer-desirable ciphersuites remain in the registries, but many TLS registries are being updated through [RFC8447], which indicates that such entries are not recommended by the IETF.)
- The integrity of the handshake depends on SHA-1 hash.
- The authentication of the peers depends on SHA-1 signatures.

⁷ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52R2.pdf>

⁸

<https://www.certicom.com/content/certicom/en/code-and-cipher/new-attack-on-rsa-based-ssl-tls-protocol.html>

⁹ <https://www.rfc-editor.org/rfc/pdf/rfc7457.txt.pdf>



- The need to support four TLS protocol versions increases the likelihood of misconfiguration.¹⁰

NSA Issues Another Notice

In January 2021, the NSA issued a bulletin strongly recommending that federal organizations replace obsolete TLS protocol configurations with updated configurations using stronger encryption and authentication to protect sensitive data.¹¹ The NSA stated that network connections using these obsolete protocols are at a higher risk of exploitation by threat actors, who can access traffic via passive decryption, modify traffic through MitM attacks, and forge certificates. Furthermore, the use of weak, compromised, unauthorized, or revoked certificates can lead to MitM attacks, regardless of whether TLS implementations are properly configured. In the bulletin, the NSA advised agencies against the use of TLS 1.0 and 1.1 specifically.

Other Attacks on TLS

In 2015, the IETF published a report titled “Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS),” which detailed several serious attacks perpetrated against TLS, including attacks on its most commonly used ciphers and modes of operation.¹²

Recommendations

- Utilize account permissions best practices, such as role-based access control, least privilege, and restricted root/admin permissions.
- Implement network segmentation using zero-trust configurations; however, given the exploitability of this vulnerability, additional security measures should also be adopted.
- Do not share passwords, and do not reuse the same password on different websites and applications.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Disable unneeded protocols on your network (UDP, IPX, NetBIOS) and monitor for any use of them.

¹⁰ ietf.org/pdf/draft-ietf-tls-oldversions-deprecate-09.pdf

¹¹

https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF

¹² <https://www.rfc-editor.org/rfc/pdfrfc/rfc7457.txt.pdf>



Appendix: Traffic Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:
RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:
RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:
AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:
AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:
GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:
GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:
WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP:
WHITE information without restriction, subject to copy-right controls.