FORTINET

OUTBREAK ALERTS

OpenSSL Buffer Overflow Vulnerability

X.509 certificate verification 4-byte buffer overflow

https://www.openssl.org/news/secadv/20221101.txt

CVEs: CVE-2022-3602

An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack in X.509 certificate verification, specifically, in name constraint checking. This buffer overflow could result in a crash which can cause a denial of service or potentially a remote code execution.

Background

OpenSSL is a full-featured Open Source Toolkit for the Transport Layer Security (TLS) protocol formerly known as the Secure Sockets Layer (SSL) protocol. It is widely used by internet servers, including the majority of HTTPS websites. Because of its widespread use and implementation, vulnerabilities in OpenSSL becomes significant in nature and could lead to information leaks. This particular issue was privately reported to OpenSSL on 17th October 2022 and users are encouraged to upgrade to a new version as soon as possible.

Announced

October 25, 2022: OpenSSL pre-announced v3.0.7, a security-fix release addressing the buffer overflow vulnerability to be released on 1st November 2022.
https://mta.openssl.org/pipermail/openssl-announce/2022-October/000238.html

Latest Developments

01 November, 2022: OpenSSL released a security advisory:
https://www.openssl.org/news/secadv/20221101.txt
01 November, 2022: OpenSSL Security Team posted a blog:
https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Weaponization

Delivery

Vulnerability

Detects and blocks endpoint attack attempts related to OpenSSL Buffer Overflow (CVE-2022-3602)

FortiClient
DB 1.353

Exploitation

IPS

Detects and blocks attack attempts related to OpenSSL Buffer Overflow (CVE-2022-3602)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 22.432	*DB 22.432*	*DB 22.432*	*DB 22.432*	*DB 22.432*

Installation

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiAnalyzer
DB 1.00074

Threat Hunting

FortiAnalyzer	FortiSIEM
v7.0+	*v6.6.0+*

Content Update

FortiSIEM
DB 308

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response	FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating	FortiRecon: EASM	FortiDevSec

Additional Resources

PSIRT	https://www.fortiguard.com/psirt/FG-IR-22-419
NIST	https://nvd.nist.gov/vuln/detail/CVE-2022-3602
OpenSSL Blog	https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/
CISA	https://www.cisa.gov/uscert/ncas/current-activity/2022/11/01/openssl-releases-security-update
Packet Storm	https://packetstormsecurity.com/files/169687/OpenSSL-Security-Advisory-20221101.html
Threat Signal	https://www.fortiguard.com/threat-signal-report/4860

Learn more about FortiGuard Outbreak Alerts