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.

October 25, 2022: OpenSSL pre-announced v3.0.7, a security-fix release addressing the buffer overflow

Announced

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/



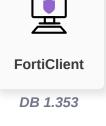
events: Reconnaissance

Weaponization

Delivery

Vulnerability

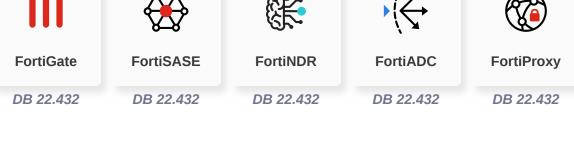
Detects and blocks endpoint attack attempts related to OpenSSL Buffer Overflow (CVE-2022-3602)



Exploitation

IPS

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



C2 Action

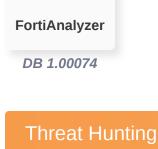
Installation

DETECT

alert and generate reports:

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

Outbreak Detection

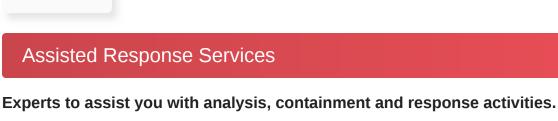






Automated Response Services that can automaticlly respond to this outbreak.

Develop containment techniques to mitigate impacts of security events:



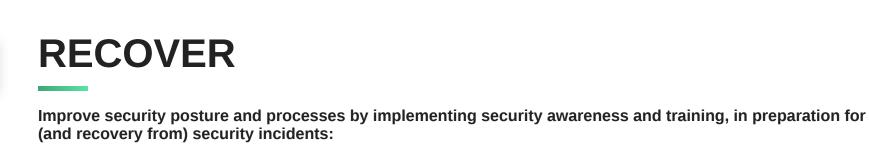
Response

FortiXDR

FortiRecon:

ACI

RESPOND



InfoSec Services

Response Readiness

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

IDENTIFY

Security reconnaissance and penetration testing services, covering both internal & external attack vectors,

Attack Surface Monitoring (Inside & Outside)

including those introduced internally via software supply chain.

Identify processes and assets that need protection:

Security FortiRecon: **FortiDevSec**



PSIRT

NIST

CISA

Rating



https://www.fortiguard.com/psirt/FG-IR-22-419

https://nvd.nist.gov/vuln/detail/CVE-2022-3602 **OpenSSL Blog**

EASM

https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/ 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