Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

Patch available for pre-announced Critical Vulnerability in OpenSSL

Date of Publication	Admiralty Code	TA Number
November 1, 2022	A1	TA2022241

Summary

OpenSSL has released the Patch for the pre-announced critical vulnerability. In the announcement the severity of the vulnerability was Critical based on the fact that it can lead to RCE but after the detailed analysis severity is downgraded to high in a security advisory published by the OpenSSL Project. This Vulnerability is about Buffer overrun in X.509 certificate verification flow, specifically in name constraint checking. Version 3.0.7 of OpenSSL fixes CVE-2022-3602 along with a similar vulnerability CVE-2022-3786.

CVEs

CVE	NAME	PATCH
CVE-2022-3602	OpenSSL X.509 Email Address 4-byte Buffer Overflow	✓
CVE-2022-3786	OpenSSL X.509 Email Address Variable Length Buffer Overflow	✓

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0042** Resource Development	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1190 Exploit Public-Facing Application	**T1566** Phishing	**TA0002** Execution	**T1203** Exploitation for Client Execution
T1587 Develop Capabilities	**T1587.003** Digital Certificates		

Technical Details

#1

On October 17, 2022, the OpenSSL Project was notified of the vulnerability. It's now identified CVE-2022-3602 and CVE-2022-3786 by OpenSSL. When a malicious client or server verifies an X.509 certificate, the vulnerability to a memory corruption bug can be exploited. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

#2

These vulnerabilities could be exploited to cause a denial of service (DoS) or remote code execution by utilizing a carefully constructed email address that makes use of non-ASCII codepoints in a client or server certificate (RCE). However, it requires that the malicious TLS certificate be signed by a trusted CA.

#3

Initially these vulnerabilities were rated as CRITICAL by OpenSSL, however now it has been downgraded to HIGH after the detail analysis. OpenSSL stated that no evidence of these vulnerabilities being exploited so far, working on the same.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-3602	OpenSSL: 3.0.0 - 3.0.6	cpe:2.3:a:openssl_software_foundation:openssl:*:*:*:*:*:*:*:*	CWE-119
CVE-2022-3786	OpenSSL: 3.0.0 - 3.0.6	cpe:2.3:a:openssl_software_foundation:openssl:*:*:*:*:*:*:*:*	CWE-119

Patch Details

Upgrade to OpenSSL version 3.0.7

References

https://www.hivepro.com/what-can-you-do-about-the-critical-vulnerability-in-openssl-3-0/
https://www.openssl.org/news/vulnerabilities.html

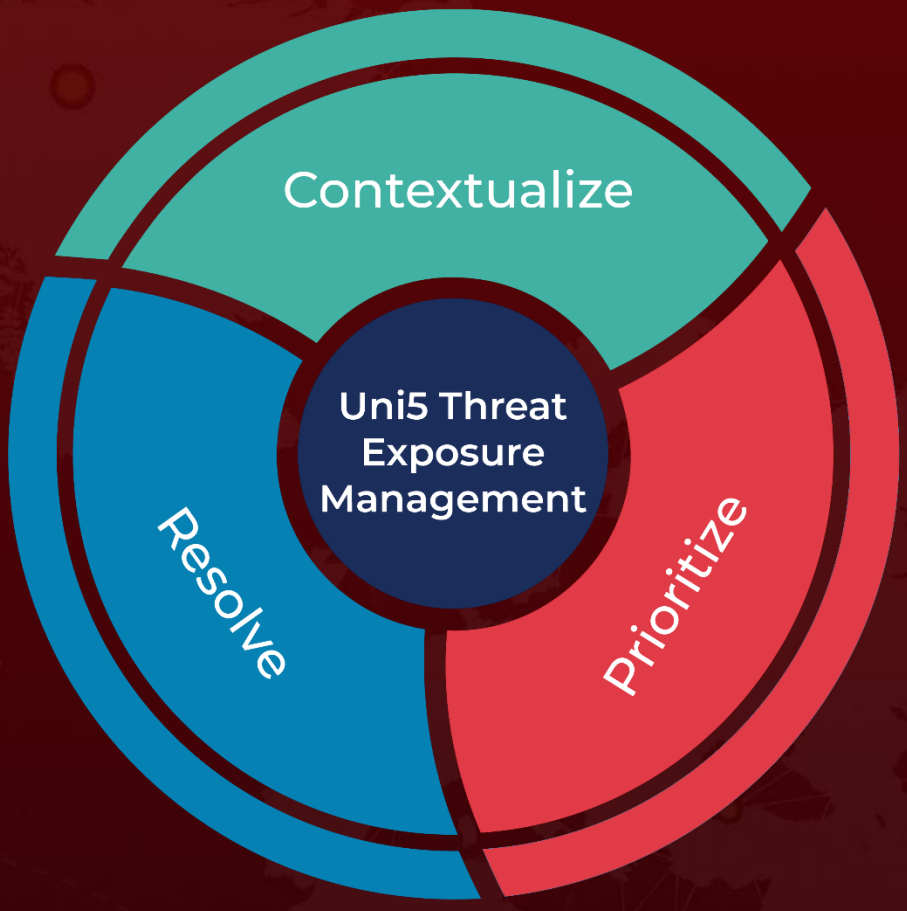
https://www.openssl.org/news/secadv/20221101.txt

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

What Next?

At **HivePro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 1, 2022 • 9:30 PM

More at www.hivepro.com