Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

OpenSSL Releases Update to Address Several High-Severity Vulnerabilities

Date of Publication	Admiralty Code	TA Number
February 09, 2023	A1	TA2023073

Summary

First Seen: January 11, 2023
Affected Product: OpenSSL
Impact: The vulnerabilities may allow an attacker to read memory contents or cause a denial-of-service.

CVEs

CVE	NAME	PATCH
CVE-2023-0286	OpenSSL X.400 address type confusion in X.509 GeneralName Vulnerability	✓
CVE-2022-4304	OpenSSL Timing Oracle in RSA Decryption Vulnerability	✓
CVE-2022-4203	OpenSSL X.509 Name Constraints Read Buffer Overflow Vulnerability	✓
CVE-2023-0215	OpenSSL Use-after-free following BIO_new_NDEF Vulnerability	✓
CVE-2022-4450	OpenSSL Double free after calling PEM_read_bio_ex Vulnerability	✓
CVE-2023-0216	OpenSSL Invalid pointer dereference in d2i_PKCS7 functions Vulnerability	✓
CVE-2023-0217	OpenSSL NULL dereference validating DSA public key Vulnerability	✓
CVE-2023-0401	OpenSSL NULL dereference during PKCS7 data verification Vulnerability	✓

Vulnerability Details

#1

The OpenSSL Project has released fixes for several security flaws, including a high-severity bug (CVE-2023-0286) that could expose users to malicious attacks. The bug is related to a type of confusion issue that may allow an attacker to read memory contents or cause a denial-of-service. The vulnerability is rooted in the way the cryptographic library handles X.509 certificates and is likely to impact only applications that have a custom implementation for retrieving a certificate revocation list.

#2

The bug has been patched in OpenSSL versions 3.0.8, 1.1.1t, and 1.0.2zg. Other security flaws addressed in the latest updates include X.509 Name Constraints Read Buffer Overflow, Timing Oracle in RSA Decryption, Double free after calling PEM_read_bio_ex, Use-after-free following BIO_new_NDEF, Invalid pointer dereference in d2i_PKCS7 functions, and NULL dereference validating DSA public key. These shortcomings could lead to an application crash, memory disclosure, and the recovery of plaintext messages sent over a network.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-0286	OpenSSL versions 3.0, 1.1.1 and 1.0.2	cpe:2.3:a:openssl_software_foundation:openssl:-:*:*:*:*:*:*:*	CWE-843
CVE-2022-4304			CWE-208
CVE-2022-4203	OpenSSL versions 3.0.0 to 3.0.7		CWE-125
CVE-2023-0215	OpenSSL versions 3.0, 1.1.1 and 1.0.2		CWE-416
CVE-2022-4450	OpenSSL versions 3.0 and 1.1.1		CWE-415
CVE-2023-0216	OpenSSL versions 3.0.0 to 3.0.7		CWE-763
CVE-2023-0217			CWE-476
CVE-2023-0401			

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' on the following pages.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0010 Exfiltration	TA0002 Execution	TA0040 Impact
TA0003 Persistence	T1499 Endpoint Denial of Service	T1106 Native API	T1030 Data Transfer Size Limits
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1140 Deobfuscate/Decode Files or Information
T1509 Command and Scripting Interpreter			

Patch Links

https://www.openssl.org/news/vulnerabilities.html

References

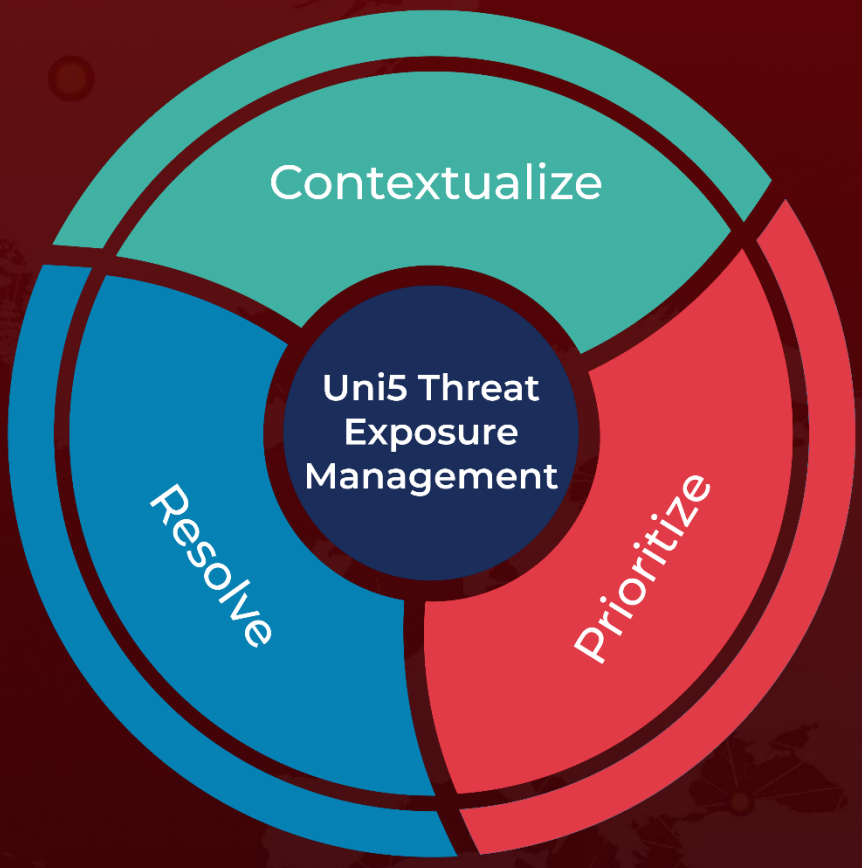
https://www.openssl.org/news/secadv/20230207.txt

https://thehackernews.com/2023/02/openssl-fixes-multiple-new-security.html

What Next?

At **Hive Pro**, 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 **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 9, 2023 • 11:30 PM

More at www.hivepro.com