Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

What can you do about the critical vulnerability in OpenSSL 3.0?

Date of Publication	Admiralty Code	TA Number
October 28, 2022	A1	TA2022237

Summary

OpenSSL has a critical vulnerability that affects all the versions from 3.0 to 3.0.6. Due to the criticality of the vulnerability, OpenSSL has pre-announced the security update for security teams to be prepared. As part of the pre-announcement, they also stated that they will release OpenSSL 3.0.7 on 1st November 2022.

CVEs

Information will be updated as soon as it's available.

Technical Details

#1

According to OpenSSL, an issue of critical severity has been found and it affects common configurations and is also likely exploitable. This vulnerability could potentially be exploited remotely to compromise server private keys or execute code. This raises concern among the security teams in order to fix it as soon as possible.

#2

The OpenSSL announcement of this vulnerability on Tuesday is likely to coincide with the release of updated versions of the technologies used by major operating system vendors, software publishers, email providers, and technology firms that have integrated OpenSSL into their goods and services. However, there will still be a huge number of people, including federal agencies, commercial businesses, service providers, network equipment makers, and innumerable website owners, who must detect the vulnerability and repair it quickly before threat actors start to take advantage of it.

Affected Products

AFFECTED OS	OpenSSL Version	AFFECTED CPE
Fedora 9	3.0	cpe:2.3:o:fedoraproject:fedora:9:*:*:*:*:*:*:*
CentOS Stream 9	3.0.1	cpe:2.3:o:centos:centos:9:*:*:*:*:*:*:*
Fedora 36	3.0.5	cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*
Fedora Rawhide	3.0.5	cpe:2.3:o:fedoraproject:fedora:rawhide:*:*:*:*:*:*:*
Kali 2022.3	3.0.5	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*
Linux Mint 21 Vanessa	3.0.2	cpe:2.3:o:linuxmint:vanessa:21:*:*:*:*:linux_mint:*:*
Mageia Cauldron	3.0.5	cpe:2.3:o:mageia:cauldron:*:*:*:*:*:*:*:*
OpenMandriva 4.3	3.0.3	cpe:2.3:o:mandriva:*:4.3:*:*:*:*:*:*:*
OpenMandriva Cooker	3.0.6	cpe:2.3:o:mandriva:*:cooker:*:*:*:*:*:*:*
Ubuntu 22.04	3.0.2	cpe:2.3:o:ubuntu:ubuntu:22.04:*:*:*:*:*:*:*
Red Hat Enterprise Linux 9	3.0	cpe:2.3:o:redhat:enterprise_linux:9.0:*:*:*:*:*:*:*
Alma Linux 9.x	3.0	cpe:2.3:o:alma:linux:9:*:*:*:*:*:*:*
Alpine Linux Edge	3.0	cpe:2.3:o:alpine:linux:*:*:*:*:*:*:*:*

Recommendations

Find all the assets, software, applications, products, etc. which use OpenSSL 3.0.x directly or indirectly and schedule a task force for those on Nov 1st, 2022, to update them to OpenSSL version 3.0.7

Patch Details

Update OpenSSL to version 3.0.7 which will be available on 1st November 2022 as stated by the vendor.

References

https://mta.openssl.org/pipermail/openssl-announce/2022-October/000238.html

https://cybersafenv.org/2022/10/27/upcoming-critical-openssl-vulnerability-what-will-be-affected-thu-oct-27th/

https://www.darkreading.com/vulnerabilities-threats/prepare-critical-flaw-openssl-security-experts-warn

https://www.openssl.org/policies/general/security-policy.html

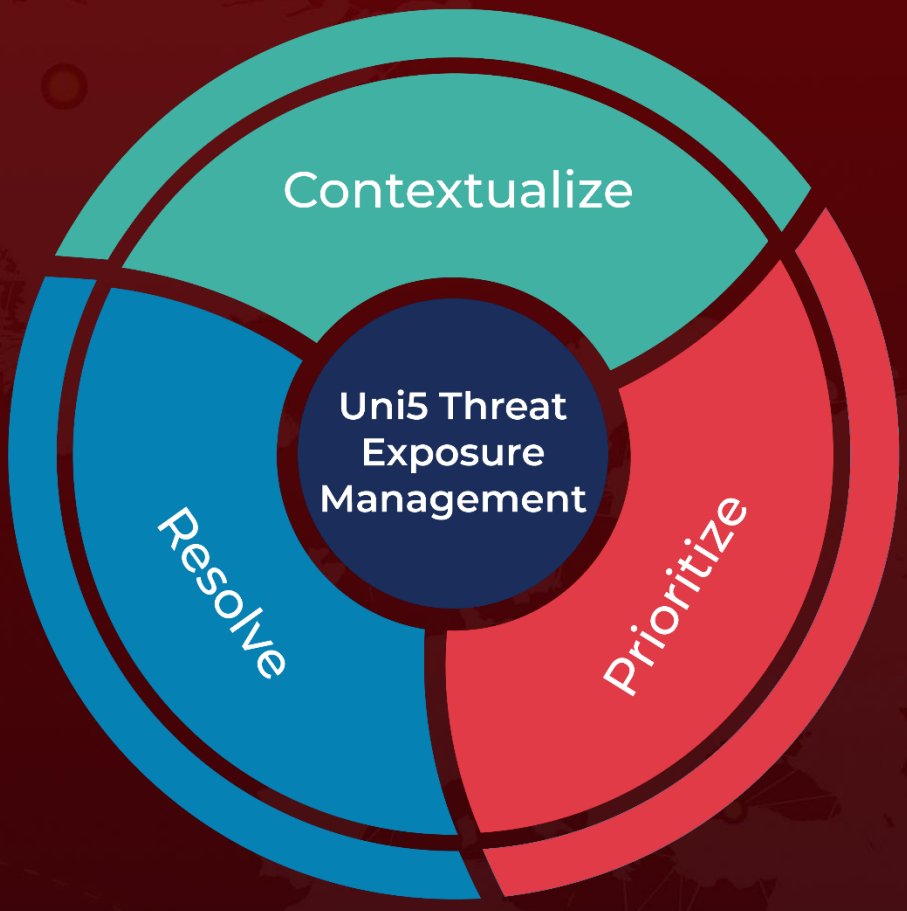
https://www.horizon3.ai/openssl-critical-vulnerability-should-you-be-spooked/

https://isc.sans.edu/forums/diary/Upcoming+Critical+OpenSSL+Vulnerability+What+will+be+Affected/29192/

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

October 28, 2022 • 3:45 AM

More at www.hivepro.com