OpenSSL 3 Critical Vulnerability | What Do Organizations Need To Do Now?

October 31, 2022
by SentinelOne

Last week, the OpenSSL project team announced the release of OpenSSL version 3.0.7, which was made available on Tuesday, November 1st. The
3.0.x, and developers and organizations are being urged to ensure that they patch any instances of OpenSSL 3 in their software stack as a matter of
2022-3602, affect version 3.0.x and do not impact OpenSSL 1.1.1 or LibreSSL.

SentinelOne customers have instant visibility of OpenSSL versions within their organizations. As such, Singularity XDR is a useful visibility solution
update.

What is OpenSSL?

OpenSSL is an open-source cryptography library widely used by applications, operating systems and websites to secure communications over the i
(Transport Layer Security). OpenSSL has been around since 2012, with version 3 released in September 2021, and is one of the most widely used c

Which Versions Of OpenSSL Are Vulnerable?

OpenSSL version 3.0.0 and higher are vulnerable to CVE-2022-3786 and CVE-2022-3602, which are patched in version 3.0.7. The majority of Oper
1.0.2; however, OpenSSL 3 is bundled with many flavors of Linux, including RedHat, Fedora, CentOS, Linux Mint and others.

Docker containers typically include some version of OpenSSL but which version and whether it is vulnerable will depend on the original configuratic
and Windows devices, although by default Macs run the unaffected LibreSSL library. Vulnerable versions of OpenSSL are also used in popular devel
and security platforms like Kali Linux.

Vulnerable

- OpenSSL 3.0.x

Not Vulnerable

- OpenSSL 1.1.1
- OpenSSL 1.1.0
- OpenSSL 1.0.2
- OpenSSL 1.0.1
- LibreSSL

What Is the Risk with OpenSSL 3 Vulnerabilities?

The OpenSSL project initially advised that a critical vulnerability in version 3.0.0 to 3.0.6 could allow for remote code execution and urged organizat
available.

That urgency remains, but since release the critical bug turned out to be two bugs, CVE-2022-3786 and CVE-2022-3602, which have been downgr
result of the bugs being more difficult to exploit than at first thought.

However, given the highly-sensitive and important nature of OpenSSL in internet communications, organizations running exposed version of OpenS
Despite the downgrading, a rating of "high" still represents a risk. It remains possible that threat actors could find ways to exploit these bugs, or res
against those that fail to patch.

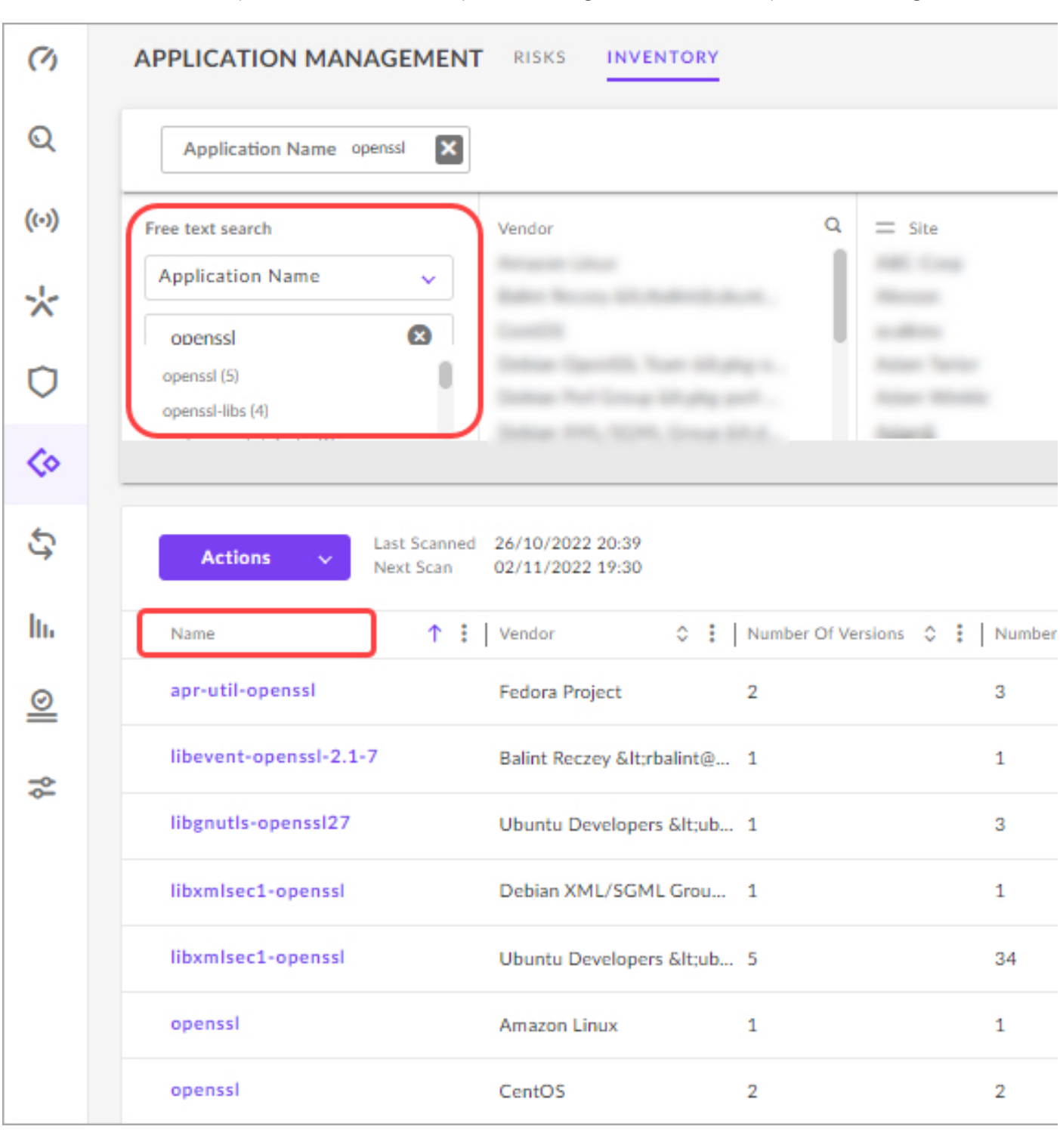
OpenSSL has suffered from a critical vulnerability before. In 2014, CVE-2014-0160, dubbed Heartbleed, was discovered in OpenSSL v1.0.1. Heart
Heartbeat Extension, which allowed more data to be read than should be allowed. In practice, the bug could be exploited to acquire passwords or e

Despite the patch being available the same day the flaw was disclosed, many were slow to patch. The bug was used to compromise a number of we
Insurance Numbers belonging to Canadian taxpayers. Even 5 years after initial disclosure, it was estimated that over 90,000 servers remained vuln

How To Prepare and Patch the OpenSSL 3 Vulnerabilities

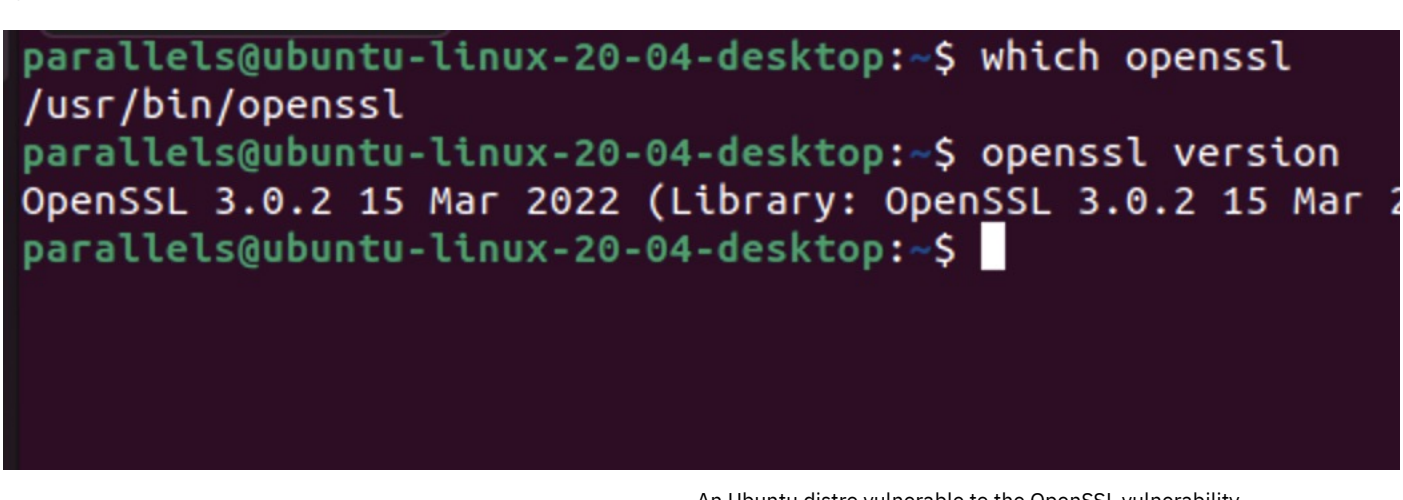
As with Heartbleed, which was rapidly exploited, organizations need to ensure that they prioritize discovering and patching CVE-2022-3786 and C\
was made available on Tuesday 1st November.

SentinelOne customers can run queries to determine which endpoints are running vulnerable versions of OpenSSL in the management console. Cus



End users can run simple queries locally to see if their operating system contains the vulnerable version.

```
openssl version
```



An Ubuntu distro vulnerable to the OpenSSL vulnerability.

Conclusion

Organizations and IT teams can become weary of patch warnings. Vulnerability discovery is at an all time high, and despite the evidence that attack
operating systems, patch management doesn't always get the time and resources it should.

Even so, vulnerabilities in a software library like OpenSSL, which is so widely in use and so fundamental to the security of data on the internet, is on
many learned in the wake of the Heartbleed bug.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Cyber War Elements In The Ukrainian Conflict | Hosted by the Alperovitch Institute for Cybersecurity Studies
- Enterprise Security Essentials | Top 15 Most Routinely Exploited Vulnerabilities 2022
- Log4j One Month On | Crimeware and Exploitation Roundup
- Staying Ahead of CVE-2022-30190 (Follina)