NCSC
National Cyber Security Centre

2211011856-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Vulnerabilities in OpenSSL
02 November 2022

Status: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

OpenSSL has released a software update that address vulnerabilities CVE-2022-3786 and CVE-2022-3602. These are both high severity vulnerabilities which can trigger buffer overruns in X.509 certificate verification. You can view the OpenSSL advisory here: https://www.openssl.org/news/vulnerabilities.html.

Products Affected

OpenSSL is used by many applications and operating systems. Any application or operating system that uses OpenSSL version 3.0.0 up to 3.0.6 is affected by this vulnerability. This may include custom applications. There is a list of common Linux distributions that include OpenSSLv3 here:

- Common Linux distributions that include OpenSSL
- Products known to be affected/unaffected by the vulnerability
- Information regarding affected Docker images

To identify whether a windows machine contains an app with OpenSSLv3 run either of the following commands:

```
C:\>dir /b/s libssl*.dll OR
Get-ChildItem -Recurse -File -ErrorAction SilentlyContinue -Path "C:\" -Filter "libssl*"
```

Impact

Exploitation of CVE-2022-3786 could allow an attacker to craft a malicious email address in a certificate that could could result in a crash (causing a denial of service).

Exploitation of CVE-2022-3602 could allow an attacker to craft a malicious email address which could result in a crash (causing a denial of service) or potentially remote code execution.

To date, there have been no reports of the active exploitation of these vulnerabilities.

Recommendations

The NCSC strongly advises affected organisations to identify any assets that are running OpenSSL version 3.x and to upgrade these to OpenSSL version 3.0.7. OpenSSL version 3.0.7 was released on Tuesday November 01. Further information and some steps that organisations can take can be found here:

- https://www.akamai.com/blog/security-research/openssl-vulnerability-how-to-effectively-prepare
- https://www.openssl.org/news/vulnerabilities.html
- https://securitylabs.datadoghq.com/articles/openssl-november-1-vulnerabilities/

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie