National Cyber Security Centre

Cyber Security Advisory

CSA-2020-1438

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

15 January 2020

The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

The severity rating for this Cyber Security Advisory is **HIGH**. This indicates the NCSC has identified activity which may pose an immediate threat to the confidentiality, integrity or availability of your IT systems. NCSC recommends any remedial actions outlined in this report are expedited to prevent or mitigate the risk associated with this activity.

Certificate Validation Vulnerability in Microsoft Windows

Details

On 15 January 2020 (NZDT), Microsoft released a security advisory detailing a vulnerability in how Windows validates digital certificates. This vulnerability has been assigned CVE number CVE-2020-0601 and affects the following versions of Windows:

- Windows 10
- Windows Server 2016 and 2019

Although Microsoft has rated the severity of this vulnerability as important, various other sources have rated it as critical with an assessment that exploitation of the vulnerability is likely to occur.

As this vulnerability affects the validation of digital certificates, it has the potential to affect any security functionality that relies on trusting certificates. This includes but is not necessarily limited to:

- TLS/HTTPS connections, potentially allowing for man-in-the-middle attacks.
- Signed executable code, potentially bypassing any restrictions based on code signing.
- Signed files and emails.

Recommendations

The NCSC recommends the relevant security updates as detailed in the "January 2020 Security Updates" release notes are applied as soon as possible to all affected Windows systems.

Priority should be given to internet facing or critical internal services that rely on TLS validation.

References:

- US National Security Agency Advisory: https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF
- Microsoft Security Response Centre CVE-2020-0601: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
- Microsoft Security Response Centre January 2020 Security Updates: https://portal.msrc.microsoft.com/en-US/security-guidance/releasenotedetail/2020-Jan

The NCSC can be contacted by email via ***info@ncsc.govt.nz****.*
We encourage you to contact us at any time if you require any further assistance or advice.