National Cyber Security Centre

Cyber Security Advisory

CSA-2020-1439

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

8 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.

Critical Vulnerability in Citrix Products

Details

In late 2019, Citrix released security bulletin CTX267027 detailing a vulnerability (CVE-2019-19781) affecting the following products:

- Citrix Application Delivery Controller (NetScaler ADC) versions 10.5, 11.1, 12.0, 12.1 and 13.0.
- Citrix Gateway (NetScaler Gateway) versions 10.5, 11.1, 12.0, 12.1 and 13.0.

Citrix has rated the severity of this vulnerability as critical, noting it allows for arbitrary code execution in affected versions of Citrix products. Exploitation of this vulnerability could result in full remote compromise of the exposed server and potentially the wider network.
Although updated firmware is not yet available to fix the vulnerability, Citrix has released mitigation steps in a separate article, CTX267679.

Recommendations

The NCSC recommends organisations using the affected products apply the mitigations detailed in Citrix article CTX267679 as soon as possible. Once a fixed version of firmware is released this should also be applied to all affected devices.

References

- Citrix security bulletin: https://support.citrix.com/article/CTX267027
- Citrix mitigation steps: https://support.citrix.com/article/CTX267679
- CVE-2019-19781: https://nvd.nist.gov/vuln/detail/CVE-2019-19781

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.