National Cyber Security Centre

Cyber Security Advisory

CSA-2020-1740

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

8 July 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 Incident Report is **HIGH**. This indicates the NCSC has identified a risk to your organisation, 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.

Remote Code Execution vulnerability in F5 BIG-IP products

Details

The National Cyber Security Centre (NCSC) is aware of a critical vulnerability affecting F5 BIG-IP products. This vulnerability has been assigned CVE number CVE-2020-5902, and allows actors with network access to the Traffic Management User Interface (TMUI), also known as the Configuration utility, to execute arbitrary commands or access credentials without authentication.

The NCSC is aware of ongoing activity in relation to this vulnerability, including widespread exploitation of internet accessible devices.

Recommendations

- Verify F5 BIG-IP devices have been updated to mitigate this vulnerability as per the guidance highlighted in the F5 Security Advisory[1].
- Restrict management interfaces such as TMUI to be only accessible from trusted networks.
- Review logging and contact the NCSC if any unauthorised access is identified.

[1] F5 Security Advisory: https://support.f5.com/csp/article/K52145254

The NCSC can be contacted by email via incidents@ncsc.govt.nz or phone ***(04) 498-7654***
We encourage you to contact us at any time if you require any further assistance or advice.