NCSC
National Cyber Security Centre

2310270115-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

F5 BIG-IP critical severity vulnerability - CVE-2023-46747

Friday 27th October, 2023

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

F5 has issued a security advisory for a critical severity vulnerability impacting their BIG-IP platform that could result in unauthenticated remote code execution. The advisory states undisclosed requests may bypass configuration utility authentication.

The issue is being tracked as CVE-2023-46747 with a CVSS score of 9.8: https://www.cve.org/CVERecord?id=CVE-2023-46747

Products Affected

The following versions of BIG-IP (all modules) are affected:

- 17.1.0
- 16.1.0 - 16.1.4
- 15.1.0 - 15.1.10
- 14.1.0 - 14.1.5
- 13.1.0 - 13.1.5

Impact

This vulnerability may allow an unauthenticated attacker with network access to the BIG-IP platform through the management port and/or self IP addresses to execute arbitrary system commands. This could lead to a total compromise of the F5 system. F5 have stated that this is a control plane issue only and there is no data plane exposure.

Recommendations

The NCSC strongly advises organisations utilising this software to identify any affected versions of BIG-IP they are running and to follow the mitigations and recommendations listed in F5's security advisory. In addition, it is recommended that users restrict access to the Traffic Management User Interface (TMUI) from the internet.

Further information and mitigation steps that organisations can take can be found here:

- https://my.f5.com/manage/s/article/K000137353

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