Security Advisory 2023-083

Critical Vulnerability in F5 BIG-IP Configuration utility

October 27, 2023 — v1.0

TLP:CLEAR

History:

- *27/10/2023 — v1.0 – Initial publication*

Summary

On 26 October 2023, F5 released a security advisory for a critical vulnerability impacting BIG-IP that allows an user to perform remote code execution. The vulnerability is tracked as **CVE-2023-46747** with a CVSS score of 9.8 out of 10. [1]

Technical Details

The **CVE-2023-46747** vulnerability may allow an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. The vulnerability resides in the Configuration utility component of the affected versions.

Affected products

All models of BIG-IP are affected.

Versions known to be vulnerable	Fixes introduced in
17.1.0	17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG
16.1.0 - 16.1.4	16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG
15.1.0 - 15.1.10	15.1.10.2 + Hotfix-BIGIP-15.1.10.2.0.44.2-ENG
14.1.0 - 14.1.5	14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG
13.1.0 - 13.1.5	13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG

Software versions that have reached the End of Technical Support (EoTS) are not listed.

Mitigations

F5 has provided a shell script specifically tailored for mitigating the identified issue on affected products version 14.1.0 and later. The script is designed to make necessary adjustments to configuration files. [1]

It is important not to run the script on software versions below 14.1.0.

Workarounds

Since the vulnerable component is the Configuration utility of the product, F5 has provided two temporary workarounds [1] which are:

- to block Configuration utility access through self IP addresses;
- to block Configuration utility access through the management interface.

Recommendations

CERT-EU strongly recommends taking one of the following actions as a priority:

1. Update to the latest version of the affected software.
2. Apply the provided mitigation and workarounds when updating is not possible immediately.

References

[1] https://my.f5.com/manage/s/article/K000137353