CERT-EU

Security Advisory 2022-080

Remote Code Execution Vulnerabilities in F5 Products

November 18, 2022 — v1.0

TLP:CLEAR

History:

- *18/11/2022 — v1.0 – Initial publication*

Summary

On November 16, 2022, F5 released an advisory on F5 Big-IP and Big-IQ concerning two CVE with high severity [1]. The first one, `CVE-2022-41622`, is a cross-site request forgery (CSRF), for which the exploitation can allow an unauthenticated attacker to perform critical actions on the system, even if the management interface is not exposed on the Internet. The second vulnerability, `CVE-2022-41800`, can allow an attacker with administrative privileges to execute arbitrary commands on the device.

Technical Details

`CVE-2022-41622` is a CSRF that requires a user with administrative rights to visit an attacker-controlled site exploiting the CSRF, while being authenticated on the F5 administrative interface. The vulnerability resides in the `/iControl/iControlPortal.cgi` SOAP endpoint which does not have proper CSRF and SOAP protections. This endpoint `iControlPortal.cgi` is a CGI script executed as root on the device and may thus lead to arbitrary execution on the system with high privileges despite the presence of SELinux [2].

`CVE-2022-41800` concerns an endpoint only accessible to administrative users, allowing to create RPM specification files then consumed by another administrator endpoint. These endpoints are vulnerable to injection, resulting in an attacker being able to add executable shell commands in the RPM spec file. These commands would then be executed when the resulting RPM file is created. A user with administrative rights might thus execute arbitrary commands on the device.

Affected Products

The following products are affected [1].

- Big-IP (all modules):
  - 17.0.0
  - 16.1.0 - 16.1.3
  - 15.1.0 - 15.1.8
  - 14.1.0 - 14.1.5
  - 13.1.0 - 13.1.5
- Big-IP SPK : All
- BIG-IQ Centralized Management:
  - 8.0.0 - 8.2.0
  - 7.1.0

Recommendations

CERT-EU recommends following the F5 advice [3]:

> *F5 has fixed this issue in an engineering hotfix that is available for supported versions of the BIG-IP system. Customers affected by this issue can request a hotfix for the latest supported versions of BIG-IP from F5 Support. To resolve this vulnerability, after installing the hotfix to one of the BIG-IP releases listed in the previous table, you must also disable Basic Authentication for iControl SOAP.*

References

[1] https://support.f5.com/csp/article/K97843387

[2] https://attackerkb.com/topics/i21EbdNxks/cve-2022-41622/rapid7-analysis

[3] https://support.f5.com/csp/article/K94221585