Security Advisory 2024-084

High Severity Vulnerabilities in F5 Products

August 21, 2024 — v1.0

TLP:CLEAR

History:

- *21/08/2024 — v1.0 – Initial publication*

Summary

On August 14, 2024, F5 released a security advisory addressing nine vulnerabilities in their products. Four of these vulnerabilities have been classified as high severity due to their potential to facilitate session hijacking and to lead to Denial-of-Service (DoS) attacks. [1,2]

Technical Details

CVE-2024-39809, with a CVSS score 8.9, is a vulnerability that facilitates session hijacking. It allows an attacker who obtains a user's session cookie to continue using that session to access the BIG-IP Next Central Manager and managed systems, even after the user logs out. This vulnerability impacts the control plane, enabling unauthorised access without affecting data plane operations [3].

CVE-2024-39778, with a CVSS score 8.7, allows a remote, unauthenticated attacker to trigger a system reboot, disrupting traffic and causing a denial-of-service (DoS) on the BIG-IP system. While this vulnerability affects the data plane by interrupting service, there is no control exposure [4].

CVE-2024-39792, with a CVSS score 8.7, allows a remote, unauthenticated attacker to degrade the performance of the NGINX service until the master and worker processes are restarted. Continued degradation can escalate into a denial-of-service (DoS). The impact is restricted to the data plane, with no exposure of the control plane [5].

CVE-2024-41727, with a CVSS score 8.7, allows a remote, unauthenticated attacker to degrade system performance by impacting the Traffic Management Microkernel (TMM) process. If the TMM process is not restarted, the degradation can result in a denial-of-service (DoS) on the BIG-IP system. This vulnerability affects only the data plane, with no exposure of the control plane [6].

Affected Products

- **CVE-2024-39809** affects BIG-IP Next Central Manager version 20.1.0.

- **CVE-2024-39778** affects BIG-IP (all modules) versions 17.1.0, 16.1.0 through 16.1.4, and 15.1.0 through 15.1.10.
- **CVE-2024-39792** affects NGINX Plus versions R30 through R32
- **CVE-2024-41727** affects BIG-IP (all modules) versions 16.1.0 through 16.1.4 and 15.1.0 through 15.1.10.

Recommendations

It is recommended applying updates to the affected assets as soon as possible.

References

[1] https://my.f5.com/manage/s/article/K000140552

[2] https://www.securityweek.com/f5-patches-high-severity-vulnerabilities-in-big-ip-nginx-plus/

[3] https://my.f5.com/manage/s/article/K000140111

[4] https://my.f5.com/manage/s/article/K05710614

[5] https://my.f5.com/manage/s/article/K000140108

[6] https://my.f5.com/manage/s/article/K000138833