February 14, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that F5 published security advisories to address vulnerabilities in the following products:

- BIG-IP – multiple versions and modules
- NGIX Plus – versions R30 and R31
- NGIX Open Source – versions 1.25.0 to 1.25.3

Technical Details

When a BIG-IP PEM classification profile is configured on a UDP virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. This issue affects classification engines using signatures released between 09-08-2022 and 02-16-2023. See the table below for a complete list of affected classification signature files. BIG-IP PEM vulnerability CVE-2024-23982 (f5.com)

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-5680 CVE-2024-23982 CVE-2024-21789 CVE-2024-23607 CVE-2024-23805 CVE-2024-23976 CVE-2024-21763 CVE-2024-23805 CVE-2024-24775 CVE-2024-23306 CVE-2024-21782 CVE-2024-23314 CVE-2024-24990 CVE-2024-24989 CVE-2024-22093 CVE-2024-23308 CVE-2024-23979 CVE-2024-24966 CVE-2024-21849 CVE-2024-21771 CVE-2024-22389 CVE-2023-48795
- F5 Security Advisories