August 15, 2024

Overall Rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of F5 vulnerabilities. The vulnerability affects BIG-IP Next Central Manager 20.x.

Technical Details

The BIG-IP Next Central Manager user session refresh token does not expire when a user logs out. An attacker with access to obtain a user's session cookies can continue to use that session to access BIG-IP Next Central Manager and systems managed by BIG-IP Next Central Manager after that user has logged out. There is no data plane exposure; this is a control plane issue only.

When a stateless virtual server is configured on a BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause virtual servers to stop processing client connections and the Traffic Management Microkernel (TMM) to terminate. Traffic is disrupted while the system automatically reboots. This vulnerability allows a remote unauthenticated attacker to cause a denial-of-service (DoS) on the BIG-IP system. There is no control plane exposure; this is a data plane issue only.

When NGINX Plus is configured to use the MQTT filter module, undisclosed requests can cause an increase in memory resource utilization. System performance can degrade until the NGINX master and worker processes are either forced to restart or are manually restarted. This vulnerability allows a remote, unauthenticated attacker to cause a degradation of service that can lead to a denial-of-service (DoS) of NGINX. There is no control plane exposure; this is a data plane issue only.

In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization. System performance can degrade until the Traffic Management Microkernel (TMM) process is either forced to restart or is manually restarted. This vulnerability allows a remote, unauthenticated attacker to cause a degradation of service that can lead to a denial-of-service (DoS) on the BIG-IP system. There is no control plane exposure; this is a data plane issue only.

When a TCP profile with Multipath TCP enabled (MPTCP) is configured on a virtual server, undisclosed traffic along with conditions beyond the attacker's control can cause the Traffic Management Microkernel (TMM) to terminate. Traffic is disrupted while the TMM process restarts. This vulnerability allows a remote unauthenticated attacker to cause a denial-of-service (DoS) on the BIG-IP system. There is no control plane exposure; this is a data plane issue only.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at VulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-39809, CVE-2024-39778, CVE-2024-39792, CVE-2024-41727, CVE-2024-41164, CVE-2024-7347, CVE-2024-41723, CVE-2024-41719,
- F5 K000140552: Quarterly Security Notification (August 2024)
- K000140111: BIG-IP Next Central Manager vulnerability CVE-2024-39809
- K05710614: BIG-IP HSB vulnerability CVE-2024-39778
- K000140108: NGINX Plus MQTT vulnerability CVE-2024-39792
- K000138833: BIG-IP TMM vulnerability CVE-2024-41727
- K000138477: BIG-IP MPTCP vulnerability CVE-2024-41164
- K000139938: BIG-IP Next Central Manager vulnerability CVE-2024-37028
- K000140529: NGINX ngx_http_mp4_module vulnerability CVE-2024-7347
- K10438187: BIG-IP iControl REST vulnerability CVE-2024-41723
- K000140006: BIG-IP Next Central Manager vulnerability CVE-2024-41719
- VRM Vulnerability Reports