May 10, 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 a F5 vulnerabilities. The vulnerability affects BIG-IP versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.4 and 15.1.0 - 15.1.10; BIG-IP Next Central Manager 20.0.1 - 20.1.0; BIG-IP (AFM) versions 17.1.0, 16.1.0 - 16.1.3 and 15.1.10; BIG-IP Next CNF BIG-IP Next CNF; BIG-IP Next Central Manager 20.0.1 - 20.0.2; BIG-IP (APM) versions 17.1.0, 16.1.0 - 16.1.4 and 15.1.0 - 15.1.10; and APM Clients 7.2.3 - 7.2.4.

Technical Details

An authenticated attacker may exploit this vulnerability by storing malicious HTML or JavaScript code in the BIG-IP Configuration utility. If successful, an attacker can run JavaScript in the context of the currently logged-in user. In the case of an administrative user with access to the Advanced Shell (bash), an attacker can leverage successful exploitation of this vulnerability to compromise the BIG-IP system. This is a control plane issue; there is no data plane exposure.

There are reports that a proof-of-concept exploit code is available for some of these vulnerabilities.

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.

References

- CVE-2024-31156, CVE-2024-21793, CVE-2024-26026, CVE-2024-33608, CVE-2024-25560, CVE-2024-32049, CVE-2024-28883, CVE-2024-33612, CVE-2024-32761, CVE-2024-33604, CVE-2024-28889, CVE-2024-27202, CVE-2024-28132
- K000139404: Quarterly Security Notification (May 2024)
- K000138636: BIG-IP Configuration utility XSS vulnerability CVE-2024-31156
- K000138732: BIG-IP Next Central Manager OData Injection vulnerability CVE-2024-21793
- K000138733: BIG-IP Next Central Manager SQL Injection vulnerability CVE-2024-26026
- K000138728: BIG-IP IPsec vulnerability CVE-2024-33608
- K000139037: TMM vulnerability CVE-2024-25560
- K000138634: BIG-IP Next Central Manager vulnerability CVE-2024-32049
- K000138744: BIG-IP APM browser network access VPN client vulnerability CVE-2024-28883
- K000139012: BIG-IP Next Central Manager vulnerability CVE-2024-33612
- K000139217: BIG-IP TMM tenants on VELOS and rSeries vulnerability CVE-2024-32761
- K000138894: BIG-IP Configuration utility XSS vulnerability CVE-2024-33604
- K000138912: BIG-IP SSL vulnerability CVE-2024-28889
- K000138520: BIG-IP Configuration utility vulnerability CVE-2024-27202

- K000138913: BIG-IP Next CNF vulnerability CVE-2024-28132
- VRM Vulnerability Reports