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 F5 published security bulletins to address vulnerabilities in the following products:

- BIG-IP – multiple versions
- BIG-IP APM – multiple versions
- BIG-IP APM Clients – versions 7.2.3 to 7.2.4

Technical Details

- K000134746: BIG-IP Edge Client for macOS vulnerability CVE-2023-38418
  The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process.

- K000133474: BIG-IP Configuration utility vulnerability CVE-2023-38138
  A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. An attacker may exploit this vulnerability by forcing an authenticated user to send a crafted URL that is then reflected and run by the user's web browser. 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.

- K000132563: BIG-IP Edge Client for Windows and macOS vulnerability CVE-2023-36858
  An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list.

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-2023-38418, CVE-2023-38138, CVE-2023-36858
- F5 Security advisory - K000135479

- F5 Security advisories