

October 26, 2023

**Overall rating: Critical**



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

## Summary

On October 26, 2023, F5 published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- BIG-IP – multiple versions and modules
- BIG-IP Next – version 20.0.1
- BIG-IP Next SPK – version 1.5.0 to 1.8.2
- BIG-IP Next CNF – version 1.1.0 to 1.1.1

## Technical Details

This vulnerability may allow an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. There is no data plane exposure; this is a control plane issue only.

This vulnerability is rated as a **Critical** 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-2023-45886, CVE-2023-46747](#)
- [F5 Security Advisory - K000137053](#)
- [F5 Security Advisory - K000137315](#)
- [F5 Security Advisories](#)

***Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.***

You will be able to find all the reports that we have published as well as all future reports here: [Cybersecurity Alerts](#)

Peter Kremer