مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High Severity Vulnerabilities in F5's BIG-IP Next Central Manager

Tracking #:432315836

Date:09-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two high-severity vulnerabilities in F5's BIG-IP Next Central Manager, if exploited, could grant an attacker admin control to the systems.

TECHNICAL DETAILS:

F5 Networks has identified and addressed high-severity vulnerabilities (CVE-2024-26026 & CVE-2024-21793) affecting BIG-IP Next Central Manager. These vulnerabilities allow unauthenticated attackers to remotely execute malicious code and gain complete administrative control over managed BIG-IP deployments. This can lead to a complete compromise of your network infrastructure, data breaches, and disruption of critical services. PoC exploit and temporary mitigation available.

Vulnerability Descriptions:

1. **CVE-2024-26026-** 7.5 HIGH - An SQL injection vulnerability exists in the BIG-IP Next Central Manager API. This allows unauthenticated attackers to inject malicious SQL code into the system, potentially leading to unauthorized access, data exfiltration, or system compromise.
2. **CVE-2024-21793**- 7.5 HIGH- An OData injection vulnerability resides within the BIG-IP Next Central Manager API. This vulnerability can be exploited by remote attackers to execute arbitrary commands on the system, granting them complete administrative control.

RECOMMENDATIONS:

- Install the latest patches provided by F5.
- Mitigation-Restrict Next Central Manager access to trusted users over a secure network to mitigate attack risks

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://my.f5.com/manage/s/article/K000138733
https://my.f5.com/manage/s/article/K000138732