Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

BIG-IP Next Central Manager Flaws Lead To Administrative Control

Date of Publication	Admiralty Code	TA Number
May 9, 2024	A2	TA2024178

Summary

Discovered: May 2024
Affected Products: BIG-IP Next Central Manager API
Impact: Two high-severity vulnerabilities, CVE-2024-26026 and CVE-2024-21793, have been identified in BIG-IP Next Central Manager. These vulnerabilities pose a risk as they can be exploited to obtain administrative control and establish covert rogue accounts on any managed assets.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-26026	BIG-IP Next Central Manager API SQL Injection Vulnerability	BIG-IP Next Central Manager API	✗	✗	✓
CVE-2024-21793	BIG-IP Next Central Manager API OData Injection Vulnerability	BIG-IP Next Central Manager API	✗	✗	✓
Unassigned	BIG-IP Next Central Manager API SSRF Vulnerability	BIG-IP Next Central Manager API	✗	✗	✗
Unassigned	BIG-IP Next Central Manager API Password Reset Vulnerability	BIG-IP Next Central Manager API	✗	✗	✗

Vulnerability Details

#1 The vulnerabilities CVE-2024-26026 and CVE-2024-21793 in F5's Next Central Manager have been uncovered, posing significant security risks by potentially granting attackers complete administrative control over the device. Additionally, these vulnerabilities may allow attackers to create accounts on any F5 assets managed by the Next Central Manager. This platform provides administrators with unified management capabilities for on-premises or cloud-based BIG-IP Next instances and services via a centralized user interface.

#2 The CVE-2024-26026 vulnerability is categorized as a SQL Injection vulnerability that exists within the device configuration. It is positioned in a way that allows potential attackers to exploit it directly for authentication bypass. An unauthenticated attacker could leverage this vulnerability to execute malicious SQL statements through the BIG-IP Next Central Manager API.

#3 On the other hand, CVE-2024-21793 exposes an OData injection vulnerability within the BIG-IP Next Central Manager API. This vulnerability stems from the Central Manager's handling of OData queries, which enables attackers to inject into an OData query filter parameter. Once injected, attackers gain sufficient leverage to extract sensitive information, such as the admin password hash, thereby escalating their privileges. Importantly, this vulnerability is contingent upon LDAP being enabled.

#4 Attackers can remotely exploit the Central Manager's management console using either CVE-2024-21793 or CVE-2024-26026, effectively gaining full administrative control. There are additional vulnerabilities which are reported but not yet assigned with CVE Ids. Of concern is that these vulnerabilities also enable new account creation which remains invisible from the Central Manager's interface. Proof-of-concept (PoC) exploits are available for two vulnerabilities, heightening the urgency of addressing these security concerns promptly.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-26026	BIG-IP Next Central Manager Versions 20.0.1 - 20.1.0	cpe:2.3:a:f5:big-ip_next_central_manager:*:*:*:*:*:*:*:*	CWE-200
CVE-2024-21793	BIG-IP Next Central Manager Versions 20.0.1 - 20.1.0	cpe:2.3:a:f5:big-ip_next_central_manager:*:*:*:*:*:*:*:*	CWE-200
Unassigned	BIG-IP Next Central Manager	cpe:2.3:a:f5:big-ip_next_central_manager:*:*:*:*:*:*:*:*	CWE-918
Unassigned	BIG-IP Next Central Manager	cpe:2.3:a:f5:big-ip_next_central_manager:*:*:*:*:*:*:*:*	-

Recommendations

Update: Kindly update your BIG-IP Next Central Manager to the latest version 20.2.0, which fixes the issues of the CVE-2024-26026 and CVE-2024-21793 vulnerabilities.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Implement a Web Application Firewall (WAF): WAF play a crucial role in detecting and mitigating SQL injection attacks. They analyze HTTP requests in real-time, looking for suspicious patterns and signatures commonly associated with SQL injection attempts. By monitoring the behavior of web applications, WAFs can identify abnormal activities indicative of an attack.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0006** Credential Access	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1190 Exploit Public-Facing Application	**T1136** Create Account	**T1212** Exploitation for Credential Access	**T1068** Exploitation for Privilege Escalation

Patch Details

Administrators should promptly update the BIG-IP Next Central Manager to version 20.2.0 to ensure that they are protected against the vulnerabilities.

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

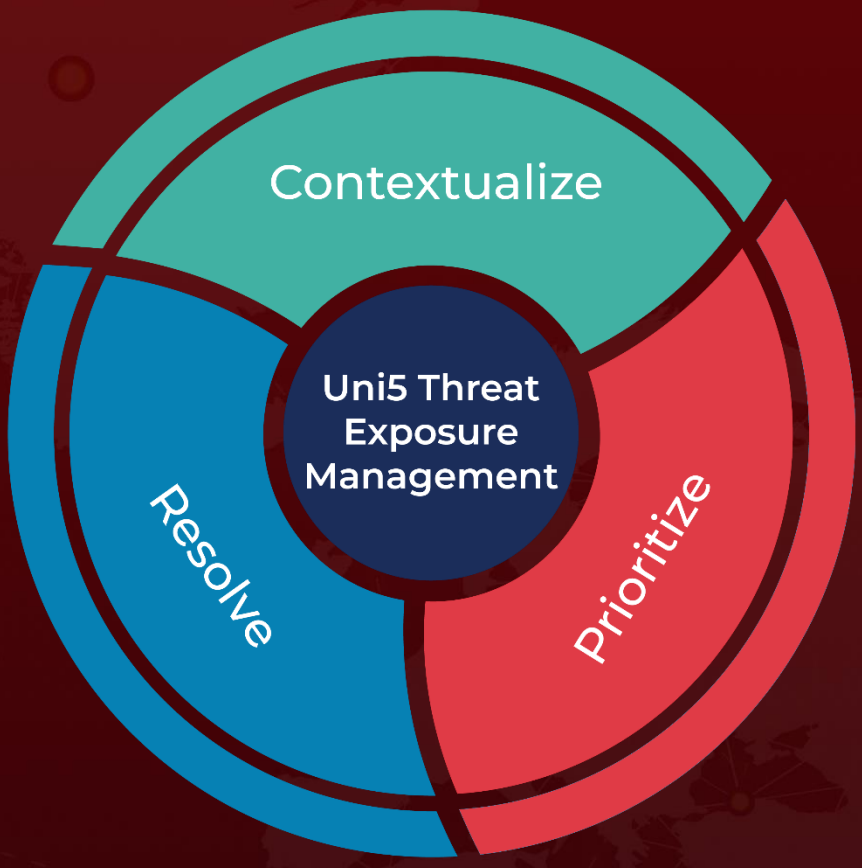
References

https://eclypsium.com/blog/big-vulnerabilities-in-next-gen-big-ip/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 9, 2024 • 6:40 AM

More at www.hivepro.com