Smarttech
YOUR 24/7 SECURITY PARTNER

Threat Report

Multiple Vulnerabilities Discovered in F5 BIG-IP Devices

9th May 2024

NSAI

QUALITY
I.S. EN ISO 27001:2013
NSAI Certified

QUALITY
I.S. EN ISO 9001:2015
NSAI Certified

Document ID	SMA- Threat Report
Document status	ISSUED
Issue Number	02
Authors	Oana Nitu < oana.nitu@smarttech247.com>
Verified by	Alin Curcan <alin.curcan@smarttech247.com>
Last modified	2024-05-09
Issue Date	2024-05-09

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e., vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed, and patches are applied before the first proof-of-concept is released.

Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time, and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Multiple vulnerabilities have been identified in F5 products, including cross-site scripting, SQL injection, and denial-of-service vulnerabilities. These vulnerabilities pose security risks to government and business entities, with potential impacts ranging from data leaks to remote code execution.

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

TECHNICAL SUMMARY:

CVE ID	**Description**
CVE-2024-31156 (BIG-IP Configuration utility XSS) **CVSS SCORE: 8.0**	• An undisclosed page within the BIG-IP Configuration utility harbors a stored cross-site scripting (XSS) vulnerability, permitting attackers to execute JavaScript within the environment of the presently authenticated user. • The exploit allows an authenticated attacker to inject harmful HTML or JavaScript code. If successful, this could enable the attacker to execute JavaScript within the context of the user currently logged in. Particularly concerning is the risk posed to administrative users with Advanced Shell (bash) access, as exploitation could compromise the entire BIG-IP system. It's important to note that this vulnerability affects the control plane exclusively, with no exposure to the data plane.

CVE-2024-21793 (BIG-IP Next Central Manager OData Injection) **CVSS SCORE: 7.5**	• A vulnerability in the BIG-IP Next Central Manager API (URI) allows for OData injection. • This vulnerability enables unauthenticated attackers to execute harmful SQL statements via the BIG-IP NEXT Central Manager API (URI).
CVE-2024-26026 (BIG-IP Next Central Manager SQL Injection) **CVSS SCORE: 7.5**	• A vulnerability involving SQL injection has been identified within the BIG-IP Next Central Manager API (URI). • An unauthenticated attacker has the capability to leverage this vulnerability to execute detrimental SQL statements via the BIG-IP Next Central Manager API (URI).
CVE-2024-33608 (BIG-IP IPsec vulnerability) **CVSS SCORE: 7.5**	• Configuring IPsec on a virtual server may result in undisclosed traffic causing the termination of the Traffic Management Microkernel (TMM). • Disruption to traffic occurs during the TMM process restart triggered by this vulnerability. It permits a remote, unauthenticated attacker to initiate a denial-of-service (DoS) attack on the BIG-IP system. Notably, this issue solely affects the data plane, with no exposure to the control plane.
CVE-2024-25560 (BIG-IP IPsec) **CVSS SCORE: 7.5**	• When BIG-IP AFM is licensed and provisioned, undisclosed DNS traffic has the potential to result in the termination of the Traffic Management Microkernel (TMM). • During the TMM process restart, traffic experiences disruption. This vulnerability enables a remote, unauthenticated attacker to initiate a denial-of-service (DoS) attack on the BIG-IP system or BIG-IP Next CNF instance. It's important to note that this issue exclusively affects the data plane, with no exposure to the control plane.
CVE-2024-32049 (BIG-IP Next Central Manager) **CVSS SCORE: 7.4**	• The BIG-IP Next Central Manager might permit an unauthenticated, remote attacker to access credentials for BIG-IP Next LTM/WAF instances. • This vulnerability could enable an unauthenticated attacker positioned in a man-in-the-middle (MITM) scenario between a BIG-IP Next LTM/WAF instance and BIG-IP Next Central Manager to decrypt and alter SSL communication between the two entities.
CVE-2024-28883 (BIG-IP APM browser network access VPN client) **CVSS SCORE: 7.4**	• An origin validation vulnerability has been identified in the BIG-IP APM browser network access VPN client, potentially enabling attackers to circumvent F5 endpoint inspection. • An unauthenticated attacker positioned in a man-in-the-middle (MITM) scenario could potentially exploit this vulnerability to establish a network access (VPN) connection with a BIG-IP APM system. This vulnerability specifically impacts the BIG-IP APM browser network access VPN client, particularly when the access policy within the Visual

	Policy Editor (VPE) of BIG-IP APM is configured with an endpoint inspection item, either client or server-side, in Endpoint Security. It's important to note that other clients like BIG-IP Edge Client, F5 Access, CLI, and similar ones remain unaffected.
CVE-2024-33612 (BIG-IP Next Central Manager) **CVSS SCORE: 6.8**	• An improper certificate validation vulnerability has been identified in BIG-IP Next Central Manager, potentially enabling attackers to impersonate an Instance Provider system. Successfully exploiting this vulnerability could facilitate crossing a security boundary. • An unauthenticated attacker in a man-in-the-middle (MITM) position could potentially exploit this vulnerability during the instantiation process to intercept and manipulate traffic between BIG-IP Next Central Manager and Instance Provider environments such as vSphere, F5 VELOS, or F5 rSeries.
CVE-2024-32761 (BIG-IP TMM tenants on VELOS and rSeries) **CVSS SCORE: 6.5**	• In specific circumstances, there's a possibility of a data leak within the Traffic Management Microkernels (TMMs) of BIG-IP tenants operating on VELOS and rSeries platforms. However, this issue cannot be exploited by attackers due to its inconsistent reproducibility and beyond their control. • This vulnerability has the potential to inadvertently disclose sensitive data to unauthorized parties.
CVE-2024-33604 (BIG-IP Configuration utility XSS) **CVSS SCORE: 6.1**	• A reflected cross-site scripting (XSS) vulnerability has been identified on an undisclosed page within the BIG-IP Configuration utility, enabling attackers to execute JavaScript within the context of the logged-in user. • This vulnerability can be exploited when an attacker manipulates an authenticated user into sending a specially crafted URL, which is then reflected and executed by the user's web browser. If successful, the attacker can execute JavaScript within the context of the logged-in user. For administrative users with access to the Advanced Shell (bash), successful exploitation of this vulnerability can compromise the entire BIG-IP system. It's important to note that this is a control plane issue and does not expose the data plane.
CVE-2024-28889 (BIG-IP SSL) **CVSS SCORE: 5.9**	• When an SSL profile with a non-default alert timeout value is set on a virtual server, undisclosed traffic and conditions outside the attacker's influence can lead to the termination of the Traffic Management Microkernel (TMM). • During the restart of the TMM process, traffic experiences disruption. This vulnerability enables a remote, unauthenticated attacker to initiate a denial-of-service (DoS) attack on the BIG-IP system.

	Importantly, this issue affects only the data plane, with no exposure to the control plane.
CVE-2024-27202 (BIG-IP Configuration utility) **CVSS SCORE: 4.7**	• There's a DOM-based cross-site scripting (XSS) vulnerability present on an undisclosed page within the BIG-IP Configuration utility. This vulnerability permits attackers to execute JavaScript within the context of the user currently logged in. • This vulnerability can be exploited when an attacker manipulates an authenticated user into visiting a malicious website that the administrator's browser perceives as being part of the same origin as the BIG-IP Configuration utility (e.g., within the same domain). If successful, the attacker can execute JavaScript within the context of the logged-in user. It's important to note that this is a control plane issue and does not expose the data plane.
CVE-2024-28132 (BIG-IP Next CNF) **CVSS SCORE: 4.4**	• A vulnerability exposing sensitive information exists within the Global Server Load Balancing (GSLB) container, potentially enabling an authenticated attacker with administrator role privileges to access this sensitive data. • An authenticated attacker has the potential to locally exploit this vulnerability via the GSLB container. If successful, the attacker can access sensitive information.

Affected Products/Version:

CVE ID	Severity	CVSS score	Affected Products	Affected versions[1]	Fixes introduced in
CVE-2024-31156	High	8.0	BIG-IP (all modules)	17.1.0 - 17.1.1 16.1.0 - 16.1.4 15.1.0 - 15.1.10	17.1.1.3 16.1.4.3 15.1.10.4
CVE-2024-21793	High	7.5	BIG-IP Next Central Manager	20.0.1 - 20.1.0	20.2.0
CVE-2024-26026	High	7.5	BIG-IP Next Central Manager	20.0.1 - 20.1.0	20.0.1 - 20.1.0
CVE-2024-33608	High	7.5	BIG-IP (all modules)	17.1.0	17.1.1
CVE-2024-25560	High	7.5	BIG-IP (AFM)	17.1.0 16.1.0 - 16.1.3 15.1.10	17.1.1 16.1.4
			BIG-IP Next CNF	1.1.0 - 1.1.1	1.2.0
CVE-2024-32049	High	7.4	BIG-IP Next Central Manager	20.0.1 - 20.0.2	20.1.0

[1] F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle.

CVE-2024-28883	High	7.4	G-IP (APM)	17.1.0 16.1.0 - 16.1.4 15.1.0 - 15.1.10	17.1.1 16.1.4.2 15.1.10.3
			APM Clients	7.2.3 - 7.2.4	7.2.4.4
CVE-2024-33612	Medium	6.8	BIG-IP Next Central Manager	20.0.1 - 20.1.0	20.2.0
CVE-2024-32761	Medium	6.5	BIG-IP (all modules)	15.1.0 - 15.1.9	15.1.10
CVE-2024-33604	Medium	6.1	BIG-IP (all modules)	17.1.0 - 17.1.1 16.1.0 - 16.1.4 15.1.0 - 15.1.10	17.1.1.3 16.1.4.3 15.1.10.4
CVE-2024-28889	Medium	5.9	BIG-IP (all modules)	17.1.0 - 17.1.1	BIG-IP (all modules)
CVE-2024-27202	Medium	4.7	BIG-IP (all modules)	17.1.0 - 17.1.1 16.1.0 - 16.1.4 15.1.0 - 15.1.10	17.1.1.3 16.1.4.3 15.1.10.4
CVE-2024-28132	Medium	4.4	BIG-IP Next CNF	1.2.0 - 1.2.1	1.3.0

***Note**: There are currently no reports of these vulnerabilities being exploited in the wild. The VPR Scores are not available at this moment.*

Recommendations

- Install a version mentioned in the "Fixes introduced in" column. If the column doesn't list a version for your branch, there's currently no available update candidate for that branch. In such cases, it is recommended to upgrade to a version that includes the fix;
- Limit management access to F5 products to trusted users and devices exclusively through a secure network;
- Turn on the automatic software update feature on your computer, mobile, and other connected devices;
- Ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats;
- Avoid clicking on links or downloading attachments in emails, especially from unknown sources and always download apps only from trusted sources;
- Apply the Principle of Least Privilege to all systems and services;
- Do not enable macros in document attachments received via emails;
- Use network intrusion detection/prevention systems to detect and prevent remote service scans;
- Ensure regular data backups are done through data backup solution to prevent data loss.

References

F5:
https://my.f5.com/manage/s/article/K000139404#exposure
https://my.f5.com/manage/s/article/K000138636
https://my.f5.com/manage/s/article/K000138732
https://my.f5.com/manage/s/article/K000138733
https://my.f5.com/manage/s/article/K000138728
https://my.f5.com/manage/s/article/K000139037
https://my.f5.com/manage/s/article/K000138634
https://my.f5.com/manage/s/article/K000138744

https://my.f5.com/manage/s/article/K000139012
https://my.f5.com/manage/s/article/K000139217
https://my.f5.com/manage/s/article/K000138894
https://my.f5.com/manage/s/article/K000138912
https://my.f5.com/manage/s/article/K000138520
https://my.f5.com/manage/s/article/K000138913

CVE List

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