مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Command Injection Vulnerability in F5 BIG-IP

Tracking #:432317254

Date:13-05-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a newly disclosed high-severity vulnerability, CVE-2025-31644, impacts F5 BIG-IP devices configured in Appliance mode that allows authenticated administrative users to exploit a command injection vulnerability via the file parameter.

TECHNICAL DETAILS:

A newly disclosed high-severity vulnerability, CVE-2025-31644, impacts F5 BIG-IP devices configured in Appliance mode. The flaw allows authenticated administrative users to exploit a command injection vulnerability via the file parameter of the save command in the iControl REST API or TMSH CLI.

Successful exploitation can result in arbitrary Bash command execution as the root user, effectively bypassing critical operational boundaries enforced by Appliance mode. This vulnerability has wide-ranging implications for control plane integrity, potential system compromise, persistence, and lateral movement.

Public proof-of-concept (PoC) code has been released, significantly increasing the risk of exploitation in unpatched systems. Organizations are strongly urged to apply patches immediately and assess systems for signs of compromise.

Vulnerability Details

- CVE ID: CVE-2025-31644
- CVSS v3.1 Base Score: 8.7 (High)
- Vector: Authenticated command injection
- Impact: Root command execution, bypass of Appliance mode shell restrictions
- Attack Vector:
  - iControl REST API (/mgmt)
  - TMSH CLI via SSH

Impacted Versions:

Product Branch	Vulnerable Versions	Fixed in Version
17.x	17.1.0 – 17.1.2	17.1.2.2
16.x	16.1.0 – 16.1.5	16.1.6
15.x	15.1.0 – 15.1.10	15.1.10.7

RECOMMENDATIONS:

- Patch Immediately: Upgrade to fixed versions.
- Restrict Access: Limit administrative access to trusted networks or through secure jump hosts.
- Monitor Logs: Look for suspicious use of the save command or API requests with abnormal file parameters.

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/K000148591