



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerabilities in F5 BIG-IP
Tracking #:432317090
Date:17-04-2025

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed high-severity vulnerabilities in F5 BIG-IP systems, which could lead to system performance degradation and potential denial-of-service (DoS) conditions on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- CVE-2025-21091 – SNMP Service Vulnerability**
 - CVSS Score 8.7 HIGH
 - When SNMP v1 or v2c is disabled, certain requests can cause a significant increase in memory utilization.
 - System performance degradation until the snmpd process is manually or forcibly restarted. This is a control plane issue and may also impact data plane traffic handling.
- CVE-2025-20058 – Message Routing Vulnerability**
 - CVSS Score 8.9 HIGH
 - Configured BIG-IP message routing profiles on virtual servers can result in memory overutilization by specific undisclosed traffic patterns.
 - Degradation of the Traffic Management Microkernel (TMM) process leading to DoS. This issue is confined to the data plane, with no control plane exposure.

Successful exploitation of this vulnerability can lead to system performance degradation, denial-of-service (DoS) conditions, and disrupted service availability, requiring manual intervention to restore normal operations.

Affected Versions:

- 17.x: 17.1.0 - 17.1.1
- 16.x: 16.1.0 - 16.1.5
- 15.x: 15.1.0 - 15.1.10

Fixed Versions:

- 17.x: 17.1.2
- 16.x: 16.1.6 Hotfix-BIGIP-16.1.5.2.0.7.5-ENG.iso
- 15.x: Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by F5.

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/K000140933?utm_source=f5support&utm_medium=RSS
- https://my.f5.com/manage/s/article/K000140947?utm_source=f5support&utm_medium=RSS