مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Critical RCE Vulnerability in F5 BIG-IP APM

Tracking #:432318690

Date:31-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability has been identified in F5 BIG-IP Access Policy Manager (APM) that allows unauthenticated Remote Code Execution (RCE).

TECHNICAL DETAILS:

A critical vulnerability has been identified in F5 BIG-IP Access Policy Manager (APM) that allows unauthenticated Remote Code Execution (RCE). Initially classified as a Denial-of-Service (DoS) issue, updated analysis in March 2026 confirms the flaw can be exploited for full system compromise.
The vulnerability carries a CVSS score of 9.8 (v3.1), indicating critical severity, and has been actively exploited in the wild. Organizations using affected versions are at significant risk, particularly where APM access policies are exposed via virtual servers.

Technical Details

- **CVE ID:** CVE-2025-53521
- **Affected Component:** apmd process (BIG-IP APM)
- **Vulnerability Type:** Remote Code Execution (RCE)
- **CWE Classification:** CWE-770 (Allocation of Resources Without Limits or Throttling)
- **Attack Vector:** Network-based (unauthenticated)
- **Exposure:** Data Plane (no control plane exposure)

Key Characteristics

- Exploitable without authentication
- Triggered via malicious traffic targeting APM-enabled virtual servers
- Impacts systems configured with access policies
- Affects appliance mode deployments
- Previously misclassified as DoS → now confirmed as RCE

Severity

- **CVSS v3.1:** 9.8 (Critical)
- **CVSS v4.0:** 9.3 (Critical)

Exploitation Status

- Confirmed **actively exploited in the wild**
- Post-compromise persistence is possible if not remediated properly

Affected Versions
Vulnerable Releases

- **17.x**
  - 17.5.0 – 17.5.1
  - 17.1.0 – 17.1.2
- **16.x**
  - 16.1.0 – 16.1.6
- **15.x**
  - 15.1.0 – 15.1.10

Fixed Versions

- **17.x:** 17.5.1.3, 17.1.3
- **16.x:** 16.1.6.1
- **15.x:** 15.1.10.8

Indicators of Compromise for c05d5254

Files on disk

- Presence of /run/bigtlog.pipe and/or /run/bigstart.ltm.
- Mismatch of file hashes when compared to known good versions of /usr/bin/umount and/or /usr/sbin/httpd.
- Mismatch of file sizes or timestamps when compared to known good versions of /usr/bin/umount and/or /usr/sbin/httpd.
- Each release and EHF may have different file sizes and timestamps.

Log entries

- /var/log/restjavad-audit.<NUMBER>.log

[ForwarderPassThroughWorker{"user":"local/f5hubblelcdadmin","method":"POST","uri":"http://localhost:8100/mgmt/tm/util/bash","status":200,"from":"Unknown"}

This entry shows a local user accessing the iControl REST API from localhost.

- /var/log/auditd/audit.log.<NUMBER>

msg='avc: received setenforce notice (enforcing=0) exe="/usr/lib/systemd/systemd" sauid=0 hostname=? addr=? terminal=?'

This entry shows a local user accessing the iControl REST API from localhost to disable SELinux.

- /var/log/audit

user=f5hubblelcdadmin folder=/Common module=(tmos)# status=[Command OK] cmd_data=run util bash <VARIABLE_COMMAND>

These log messages show an echo of Base64-encoded data written into a file and the execution of /run/bigstart.ltm. This entry shows an example of a command being run in the audit log, correlated to the iControl REST request above.

Command output

- sys-eicheck

There is a failure of sys-eicheck, especially /usr/bin/umount and/or /usr/sbin/httpd. The system integrity checker sys-eicheck is a software component installed on BIG-IP. It relies upon the RPM integrity check functionality and reconciles on-disk executable files with hashes in the RPM database. When the tool is run and a mismatch is detected, users are alerted. We have observed a threat actor making modifications to the underlying components which sys-eicheck relies upon to perform its checks. Our understanding at this time is that the threat actor modified these components in one partition (original running version compromised) but failed to make the same modifications on the second partition (destination for upgrade). When the customer upgraded and rebooted into the second partition, the modifications to sys-eicheck components did not persist.

- lsof -n

The output of this command contains entries for /run/bigtlog.pipe.

TTPs

- You may observe HTTP/S traffic from the BIG-IP system that contains HTTP 201 response codes and CSS content-type to disguise the attacker's activities.
- Changes to the following files might signal a potential compromise; however, their presence alone does not indicate a security issue:
  - /var/sam/www/webtop/renderer/apm_css.php3
  - /var/sam/www/webtop/renderer/full_wt.php3
  - /var/sam/www/webtop/renderer/webtop_popup_css.php3

RECOMMENDATIONS:

- Immediate Actions
  - Upgrade immediately to a fixed version.
- Threat Hunting & Validation
  - Review Indicators of Compromise (IoCs) (K000160486)

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/K000156741
- https://my.f5.com/manage/s/article/K000160486