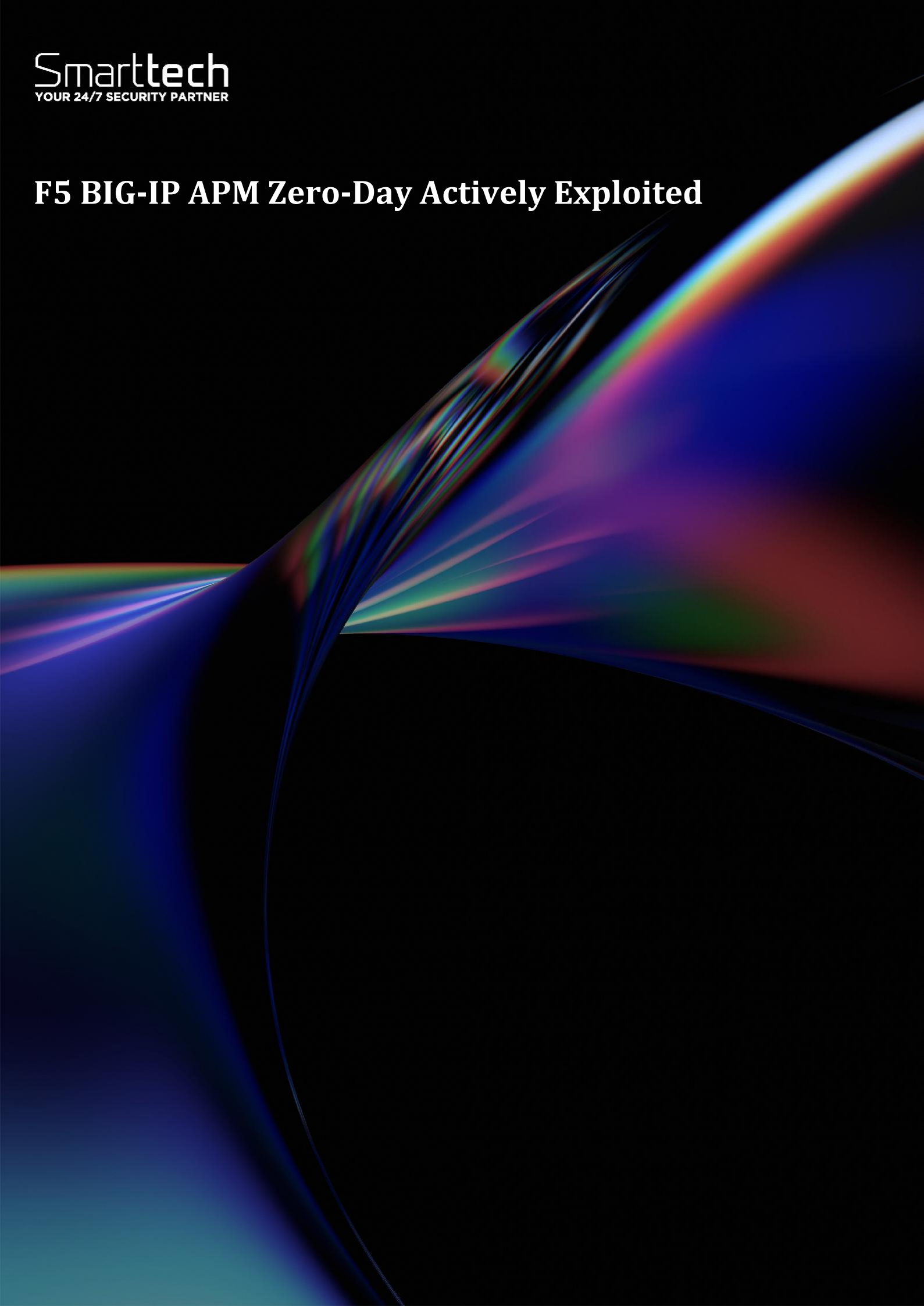


F5 BIG-IP APM Zero-Day Actively Exploited



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	169
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-23
Issue Date	2026-09-22

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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

A critical severity vulnerability in F5 BIG-IP Access Policy Manager (APM) allows for remote code execution and is actively exploited in the wild as zero-day. BIG-IP APM is a widely deployed network access and identity management solution used across government agencies, financial institutions, healthcare organizations, and large enterprises to control application and network access. Successful exploitation of this vulnerability could result in an attacker gaining full control of the affected system. Depending on the privileges associated with the account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Accounts configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

Risk

Government:

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

Businesses:

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

Technical summary

The vulnerability, identified as **CVE-2026-94127**, affects the Access Policy Manager (APM) component of F5 BIG-IP and is associated with a CVSS score of 9.3

When a BIG-IP APM access policy and an OAuth profile is configured on a virtual server, specific malicious traffic can lead to Remote Code Execution (RCE). This vulnerability allows an unauthenticated attacker to perform remote code execution. The BIG-IP system in Appliance mode is also vulnerable. This is a data plane issue, there is no control plane exposure.

This vulnerability may allow an attacker to gain full control of the affected system.

The vulnerability is actively exploited and has been added to CISA's KEV catalog, making it a priority for immediate remediation.

Affected Products

- F5 BIG-IP (APM module) version 21.1.0
- F5 BIG-IP (APM module) versions 17.5.0 - 17.5.1
- F5 BIG-IP (APM module) versions 17.1.0 - 17.1.3

Indicators of Compromise

Three indicators observed close in time to one another should be considered a reason to investigate further. Presence of these indicators alone does not necessarily mean there is an issue, but combination and frequency have been seen to correlate with an attack.

At a high level, multiple OAuth authentication failures, followed by suspicious commands, shortly followed by a TMM SIGABRT is the combination that should lead to human review of the system.

- OAuth failures
 - This is a medium confidence indicator of attack. The log message is normal to observe in some situations, so the signal here is repetition not presence. Sustained repetition (≥ 10 in one log) is the anomaly a human should review, especially if all observed from a single IP address. While the log message presence alone does not confirm compromise, it should be considered as potential indicator of attack.
- Log messages
 - /var/log/apm
 - <DATE> <HOST> err tmm1[30975]: 01990004:3: <PROFILE_NAME>: Request UserInfo from Source ID (null) IP <IP> failed. Error Code (invalid_token) Error Description (The access token is invalid.)
- TMCTL statistics
 - The following command will output the statistics for BIG-IP APM OAuth failures. An unexplained increase in total_failed should be investigated further:
\$ tmctl global_oauth_stat -s total_requests,total_userinfo_requests,total_failed
- Audit log entries
 - /var/log/audit

If the log oauth failures messages above are noticed, especially in rapid succession or large volume, the time stamps should be noted, and audit logs should be investigated around those time stamps.

- TMM core file presence
 - We have observed TMM enters a loop, which causes the SOD daemon to send a SIGABRT. Presence of a TMM core file alone is not an indicator, but core files should be investigated.

Mitigation

To mitigate this vulnerability, you can apply an iRule to the affected BIG-IP APM virtual server. Contact [F5 Support](#) to obtain the iRule.

Recommendations

The **Smarttech247 team** recommends the following actions:

- Apply appropriate workarounds provided by F5 to vulnerable systems immediately after appropriate testing. ([M1051: Update Software](#))
 - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
 - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and

- maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
- **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. ([M1026: Privileged Account Management](#))
 - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include disabling default accounts or making them unusable.
 - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. ([M1016: Vulnerability Scanning](#))
 - **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate

critical cloud systems. (**M1030: Network Segmentation**)

- **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
 - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

<https://my.f5.com/manage/s/article/K000162605>

<https://www.bleepingcomputer.com/news/security/f5-warns-of-big-ip-apm-remote-code-execution-zero-day-exploited-in-attacks/>

CVE

CVE-2026-94127

