An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2603311419

NCSC Advisory

F5 BIG-IP Vulnerability Reclassified as RCE, Under Exploitation

CVE-2025-53521

31st, March 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2025-53521

Published: 2025-10-15

Vendor: F5

Product: BIG-IP

CVSS Score[1]: 9.8

Products Affected

Product	Version
BIG-IP	17.5.0 < 17.5.1.3
BIG-IP	17.1.0 < 17.1.3
BIG-IP	16.1.0 < 16.1.6.1
BIG-IP	15.1.0 < 15.1.10.8

Impact

When a BIG-IP APM access policy is configured on a virtual server, specific malicious traffic can lead to Remote Code Execution (RCE).

Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

This vulnerability was originally published in October 2025 but recent events and related information have required a reassessment and a republication of the vulnerability.

Common Weakness Enumeration (CWE)[2]: CWE-770: CWE-770 Allocation of Resources Without Limits or Throttling

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from F5.

The patch for this vulnerability that was released in October is still valid and will protect from exploitation.

As a timeline for exploitation of this vulnerability is not yet available it is expected that some exploitation was/could have been occurring prior to the initial vulnerability and patch publication, it is therefore the NCSC's advice that you follow the following recommendations:

Use F5's buitin utility sys-eicheck to check the system for integrity issues.

Use F5's builtin utility qkview to submit a report to F5, F5 can use heuristics to identify compromises. When you have submitted a report to F5 using qkview they recommend that you raise an associated case which will allow a quicker and more thorough response process. The following articles includes the indicators of compromise associated with known exploitations and instructions on sys-eicheck

https://my.f5.com/manage/s/article/K00029945

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

- https://nvd.nist.gov/vuln/detail/CVE-2025-53521
- https://www.cve.org/CVERecord?id=CVE-2025-53521
- https://my.f5.com/manage/s/article/K000156741
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-53521