Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0386

Kwetsbaarheid verholpen in F5 Networks BIG-IP Access Policy Manager

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 23-09-2026
Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

F5 Networks heeft aangegeven dat systemen alleen kwetsbaar zijn wanneer deze als OAuth Authorisation Server zijn geconfigureerd. Dit is aan deze securityadvisory toegevoegd. De inschaling van deze advisory blijft ongewijzigd HIGH/HIGH.

Feiten

F5 Networks heeft een kwetsbaarheid verholpen in BIG-IP Access Policy Manager (APM).

Duiding

De kwetsbaarheid stelt een ongeauthenticeerde kwaadwillende in staat om malafide code uit te voeren. Hiertoe dient de kwaadwillende malafide netwerkverkeer naar het kwetsbare systeem te versturen. BIG-IP APM-systemen zijn alleen kwetsbaar wanneer een access policy is geconfigureerd en het systeem dienstdoet als OAuth Authorisation Server.

F5 Networks geeft aan dat het een zeroday-kwetsbaarheid is die actief wordt misbruikt.

Oplossingen

F5 Networks heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Ook heeft F5 indicators-of-compromise (IOC's) gepubliceerd. Het NCSC adviseert organisaties met klem om kwetsbare systemen op aanwezigheid van deze IOC's te controleren alvorens de beveiligingsupdates worden geïnstalleerd. Met het oog op actief misbruik van de kwetsbaarheid, raadt het NCSC aan om dit zo spoedig mogelijk te doen.

Voor organisaties die niet in de gelegenheid zijn om de updates op korte termijn te installeren, heeft F5 Networks andere mitigerende maatregelen beschikbaar. Lees het beveiligingsadvies van F5 Networks voor meer informatie.

Referenties

- https://my.f5.com/manage/s/article/K000162605

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-94127	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow

Getroffen producten

F5
BIG-IP (APM)

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.