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: 22-09-2026

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

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 en een OAuth-profiel op de virtuele server zijn geconfigureerd.

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, raad 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