Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0508

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in F5 BIG-IP

Publicatiedatum: 19-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

F5 heeft meerdere kwetsbaarheden verholpen in F5 BIG-IP, specifiek in componenten zoals de Traffic Management Microkernel (TMM), iControl REST interface, iControl SOAP utility en Access Policy Manager (APM).

Duiding

De kwetsbaarheden bevinden zich voornamelijk in de Traffic Management Microkernel (TMM) die verantwoordelijk is voor de data plane van F5 BIG-IP systemen. Diverse commando's en functies binnen iRules, zoals GENERICMESSAGE::route, PSC::ip_address, MR::message route, DNS::scrape en PEM::subscriber, kunnen een crash van de TMM veroorzaken, wat leidt tot denial-of-service (DoS) condities en verstoring van netwerkverkeer. Sommige van deze kwetsbaarheden kunnen door een niet-geauthenticeerde aanvaller worden misbruikt om op afstand willekeurige code uit te voeren. Daarnaast is er een kwetsbaarheid in de iControl REST interface waarbij uitgegeven tokens niet automatisch verlopen, waardoor een aanvaller met toegang tot een token de geldigheid ervan onbeperkt kan verlengen. In de iControl SOAP interface kan een geauthenticeerde gebruiker met minimaal Guest-toegang onbevoegde managementverzoeken injecteren en systeemcommando's uitvoeren, wat de control plane beïnvloedt. Verder zijn er kwetsbaarheden in de Access Policy Manager (APM) die, onder bepaalde configuraties zoals per-request policies, form-based logon pages en SAML SP agent met encrypted assertions, kunnen leiden tot onverwachte beëindiging van de TMM en daarmee DoS-condities op de data plane.

Oplossingen

F5 heeft updates uitgebracht om de kwetsbaarheden in BIG-IP te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://my.f5.com/manage/s/article/K000163929
- https://my.f5.com/manage/s/article/K000163936
- https://my.f5.com/manage/s/article/K000163937
- https://my.f5.com/manage/s/article/K000163938
- https://my.f5.com/manage/s/article/K000163939
- https://my.f5.com/manage/s/article/K000163940
- https://my.f5.com/manage/s/article/K000163941
- https://my.f5.com/manage/s/article/K000163942
- https://my.f5.com/manage/s/article/K000163943

- https://my.f5.com/manage/s/article/K000163944
- https://my.f5.com/manage/s/article/K000163945
- https://my.f5.com/manage/s/article/K000163946
- https://my.f5.com/manage/s/article/K000164058

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-116953	9.3 CRITICAL
CVE-2026-120285	9.3 CRITICAL
CVE-2026-120292	9.3 CRITICAL
CVE-2026-120718	9.2 CRITICAL
CVE-2026-120722	9.3 CRITICAL
CVE-2026-121805	9.3 CRITICAL
CVE-2026-121812	8.7 HIGH
CVE-2026-123637	9.3 CRITICAL
CVE-2026-125272	8.7 HIGH
CVE-2026-125274	8.7 HIGH
CVE-2026-126336	8.7 HIGH
CVE-2026-126822	8.7 HIGH

CWE's

CWE	Beschrijving
CWE-93	Improper Neutralization of CRLF Sequences
CWE-121	Stack-based Buffer Overflow
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-1463	Insufficient Session Timeout Value

Getroffen producten

F5
BIG-IP
BIG-IP (all modules)
BIG-IP APM
BIG-IP Access Policy Manager
BIG-IP CNF
BIG-IP Next for Kubernetes
BIG-IP SSL Orchestrator

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.