Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0162

Kwetsbaarheden verholpen in F5 BIG-IP en BIG-IQ producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-05-2026

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 heeft meerdere kwetsbaarheden verholpen in de BIG-IP en BIG-IQ productlijnen, inclusief componenten zoals iControl REST, iControl SOAP, TMOS Shell, Traffic Management Microkernel (TMM), Configuration utility, Advanced WAF, ASM, PEM, DNS, Access Policy Manager (APM) en SSL Orchestrator.

Duiding

De kwetsbaarheden betreffen onder andere directory traversal, ongeautoriseerde bestandswijzigingen, blootstelling van gevoelige SSH-wachtwoorden in API-responses en auditlogs, privilege escalatie via onjuiste permissie-toewijzingen, remote command injection, cross-account informatielekken, en onverwachte procesafsluitingen (zoals van TMM, httpd, apmd en bd processen) door specifieke configuraties of ongedocumenteerde verkeerspatronen.

Exploitatie vereist doorgaans geauthenticeerde toegang met rollen variërend van Manager, Resource Administrator tot Administrator, afhankelijk van de kwetsbaarheid. Sommige kwetsbaarheden maken het mogelijk om configuratieobjecten te wijzigen, wat kan leiden tot het uitvoeren van willekeurige commando's met verhoogde privileges.

Andere kwetsbaarheden betreffen het lekken van gevoelige informatie via onjuiste toegangscontrole of onvoldoende validatie binnen managementinterfaces. Diverse kwetsbaarheden zijn specifiek voor Appliance mode of bepaalde configuratieprofielen zoals SSL, HTTP/2, SIP, LDAP authenticatie, en SNMP configuraties. De impact omvat onder meer het omzeilen van beveiligingscontroles, het escaleren van privileges, het lekken van gevoelige gegevens, en het verstoren van de beschikbaarheid en stabiliteit van netwerk- en applicatiebeheercomponenten. Niet-ondersteunde softwareversies zijn in de meeste gevallen niet geëvalueerd voor deze kwetsbaarheden.

Oplossingen

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

Referenties

- https://my.f5.com/manage/s/article/K000160975
- https://my.f5.com/manage/s/article/K000160979
- https://my.f5.com/manage/s/article/K000160981
- https://my.f5.com/manage/s/article/K000161018
- https://my.f5.com/manage/s/article/K000161022
- https://my.f5.com/manage/s/article/K000161023
- https://my.f5.com/manage/s/article/K000161040

- https://my.f5.com/manage/s/article/K000161056
- https://my.f5.com/manage/s/article/K000161107
- https://my.f5.com/manage/s/article/K000149743
- https://my.f5.com/manage/s/article/K000156581
- https://my.f5.com/manage/s/article/K000156604
- https://my.f5.com/manage/s/article/K000156761
- https://my.f5.com/manage/s/article/K000156734
- https://my.f5.com/manage/s/article/K000157895
- https://my.f5.com/manage/s/article/K000157981
- https://my.f5.com/manage/s/article/K000158038
- https://my.f5.com/manage/s/article/K000158070
- https://my.f5.com/manage/s/article/K000158082
- https://my.f5.com/manage/s/article/K000158971
- https://my.f5.com/manage/s/article/K000158978
- https://my.f5.com/manage/s/article/K000158979
- https://my.f5.com/manage/s/article/K000159021
- https://my.f5.com/manage/s/article/K000159034
- https://my.f5.com/manage/s/article/K000160727
- https://my.f5.com/manage/s/article/K000160788
- https://my.f5.com/manage/s/article/K000160857
- https://my.f5.com/manage/s/article/K000160862
- https://my.f5.com/manage/s/article/K000160863
- https://my.f5.com/manage/s/article/K000160874
- https://my.f5.com/manage/s/article/K000160875
- https://my.f5.com/manage/s/article/K000160876
- https://my.f5.com/manage/s/article/K000160901
- https://my.f5.com/manage/s/article/K000160903
- https://my.f5.com/manage/s/article/K000160911
- https://my.f5.com/manage/s/article/K000160916
- https://my.f5.com/manage/s/article/K000160926
- https://my.f5.com/manage/s/article/K000160945
- https://my.f5.com/manage/s/article/K000160971
- https://my.f5.com/manage/s/article/K000160972
- https://my.f5.com/manage/s/article/K000160973

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-24464	**6.9 MEDIUM**

CVE-2026-28758	6.7 MEDIUM
CVE-2026-32643	8.5 HIGH
CVE-2026-32673	8.5 HIGH
CVE-2026-34176	8.5 HIGH
CVE-2026-35062	7.1 HIGH
CVE-2026-39455	8.7 HIGH
CVE-2026-39458	8.7 HIGH
CVE-2026-39459	8.6 HIGH
CVE-2026-40060	8.7 HIGH
CVE-2026-40061	8.5 HIGH
CVE-2026-40067	8.7 HIGH
CVE-2026-40423	8.7 HIGH
CVE-2026-40435	6.9 MEDIUM
CVE-2026-40462	7.1 HIGH
CVE-2026-40618	8.7 HIGH
CVE-2026-40629	8.7 HIGH
CVE-2026-40631	8.5 HIGH
CVE-2026-40698	8.5 HIGH
CVE-2026-40699	7.1 HIGH
CVE-2026-40703	5.3 MEDIUM
CVE-2026-41217	8.3 HIGH
CVE-2026-41218	8.7 HIGH
CVE-2026-41219	7.1 HIGH

CVE-2026-41225	8.6 HIGH
CVE-2026-41227	8.7 HIGH
CVE-2026-41953	8.5 HIGH
CVE-2026-41954	6.9 MEDIUM
CVE-2026-41956	8.7 HIGH
CVE-2026-41957	8.7 HIGH
CVE-2026-41959	7.1 HIGH
CVE-2026-42058	5.3 MEDIUM
CVE-2026-42063	6.9 MEDIUM
CVE-2026-42406	8.5 HIGH
CVE-2026-42408	6.7 MEDIUM
CVE-2026-42409	8.7 HIGH
CVE-2026-42780	6.9 MEDIUM
CVE-2026-42781	7.1 HIGH
CVE-2026-42919	7.1 HIGH
CVE-2026-42920	8.7 HIGH
CVE-2026-42924	8.5 HIGH
CVE-2026-42930	8.5 HIGH
CVE-2026-42937	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-35	Path Traversal: '.../...//'
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-131	Incorrect Calculation of Buffer Size
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-250	Execution with Unnecessary Privileges
CWE-252	Unchecked Return Value
CWE-266	Incorrect Privilege Assignment
CWE-267	Privilege Defined With Unsafe Actions
CWE-272	Least Privilege Violation
CWE-312	Cleartext Storage of Sensitive Information
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-416	Use After Free
CWE-420	Unprotected Alternate Channel
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data
CWE-532	Insertion of Sensitive Information into Log File
CWE-552	Files or Directories Accessible to External Parties
CWE-643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')
CWE-648	Incorrect Use of Privileged APIs
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime

CWE-824	Access of Uninitialized Pointer
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

Getroffen producten

F5
AI Gateway
BIG- IP
BIG-IP APM
BIG-IP Advanced WAF/ASM
BIG-IP Advanced WAF/ASM and BIG-IP DDoS Hybrid Defender
BIG-IP DNS
BIG-IP Next CNF
BIG-IP Next SPK
BIG-IP Next for Kubernetes
BIG-IP PEM
BIG-IP SSL Orchestrator
BIG-IP tenants on BX110 blades on VELOS
BIG-IP tenants on BX520 blades on VELOS

BIG-IP tenants on all other rSeries systems
BIG-IP tenants on r10000 rSeries
BIG-IP tenants on r12000 rSeries
BIG-IP tenants on r5000 rSeries
BIG-IQ
BIG-IQ Centralized Management
Distributed Cloud (all services)
NGINX (all products)
OS-A
OS-C
SSL Orchestrator
Silverline (all services)
Traffix SDC

Disclaimer