



NCSC-2025-0319

Kwetsbaarheden verholpen in F5 Networks BIG-IP, F5OS en NGINX App Protect WAF

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-10-2025

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 kwetsbaarheden verholpen in de BIG-IP- en F5OS-productlijnen en NGINX App Protect WAF.

Duiding

De kwetsbaarheden omvatten verschillende configuratieproblemen en exploitatievectoren. Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service
- Manipulatie van gegevens
- Uitvoeren van willekeurige code (root/adminrechten)
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten

Oplossingen

F5 Networks heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Aanvullend op bovengenoemd beveiligingsadvies heeft F5 Networks een websitebericht gepubliceerd over een beveiligingsincident op hun systemen. F5 Networks adviseert klanten hierin de laatste beveiligingsupdates zo snel mogelijk te installeren. Daarnaast heeft F5 Networks detectie- en hardeningmaatregelen gedeeld, en adviseert het bedrijf deze maatregelen in te zetten. Lees het websitebericht voor meer informatie.

Referenties

- <https://my.f5.com/manage/s/article/K000154696>
- <https://my.f5.com/manage/s/article/K000156572>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-61938	8.7 HIGH
➤ CVE-2025-54858	8.7 HIGH
➤ CVE-2025-58120	8.7 HIGH

> CVE-2025-53856	8.7 HIGH
> CVE-2025-61974	8.7 HIGH
> CVE-2025-58071	7.5 HIGH
> CVE-2025-53521	8.7 HIGH
> CVE-2025-61960	8.7 HIGH
> CVE-2025-54854	8.7 HIGH
> CVE-2025-53474	8.7 HIGH
> CVE-2025-61990	7.5 HIGH
> CVE-2025-61935	7.5 HIGH
> CVE-2025-59778	7.7 HIGH
> CVE-2025-59481	8.5 HIGH
> CVE-2025-61958	8.5 HIGH
> CVE-2025-47148	7.1 HIGH
> CVE-2025-47150	7.1 HIGH
> CVE-2025-55670	7.1 HIGH
> CVE-2025-54805	6.0 MEDIUM
> CVE-2025-59269	8.4 HIGH
> CVE-2025-58153	8.2 HIGH
> CVE-2025-53868	8.5 HIGH
> CVE-2025-61955	8.5 HIGH
> CVE-2025-57780	7.8 HIGH
> CVE-2025-60016	8.7 HIGH
> CVE-2025-48008	8.7 HIGH

> CVE-2025-59781	8.7 HIGH
> CVE-2025-41430	8.7 HIGH
> CVE-2025-55669	8.7 HIGH
> CVE-2025-61951	8.7 HIGH
> CVE-2025-55036	8.7 HIGH
> CVE-2025-54479	8.7 HIGH
> CVE-2025-46706	8.7 HIGH
> CVE-2025-59478	8.7 HIGH
> CVE-2025-60015	6.9 MEDIUM
> CVE-2025-59483	8.5 HIGH
> CVE-2025-60013	4.6 MEDIUM
> CVE-2025-59268	6.9 MEDIUM
> CVE-2025-58474	6.9 MEDIUM
> CVE-2025-61933	6.1 MEDIUM
> CVE-2025-54755	6.9 MEDIUM
> CVE-2025-53860	4.1 MEDIUM
> CVE-2025-58424	6.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-73	External Control of File Name or Path
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-79	

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	
> CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
> CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CWE-125	Out-of-bounds Read
> CWE-146	Improper Neutralization of Expression/Command Delimiters
> CWE-201	Insertion of Sensitive Information Into Sent Data
> CWE-214	Invocation of Process Using Visible Sensitive Information
> CWE-250	Execution with Unnecessary Privileges
> CWE-252	Unchecked Return Value
> CWE-340	Generation of Predictable Numbers or Identifiers
> CWE-401	Missing Release of Memory after Effective Lifetime
> CWE-404	Improper Resource Shutdown or Release
> CWE-415	Double Free
> CWE-416	Use After Free
> CWE-425	Direct Request ('Forced Browsing')
> CWE-457	Use of Uninitialized Variable
> CWE-459	Incomplete Cleanup
> CWE-476	NULL Pointer Dereference
> CWE-672	Operation on a Resource after Expiration or Release
> CWE-674	Uncontrolled Recursion
> CWE-703	Improper Check or Handling of Exceptional Conditions
> CWE-705	Incorrect Control Flow Scoping
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-787	Out-of-bounds Write

➤ CWE-824	Access of Uninitialized Pointer
➤ CWE-1284	Improper Validation of Specified Quantity in Input

Getroffen producten

F5
BIG-IP
F5OS - Appliance
F5OS - Chassis
F5OS- A
F5OS- C
NGINX
NGINX App Protect WAF

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.