



NCSC-2025-0041

Kwetsbaarheden verholpen in F5 BIG-IP

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-02-2025

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

Door een technisch issue is deze advisory eerder verstuurd met een invalide signature, waardoor automatische verwerking mogelijk verstoord is. Deze update verhelpt dat. Er is verder geen inhoudelijke wijziging.

Feiten

F5 heeft kwetsbaarheden verholpen in BIG-IP.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Omzeilen van een beveiligingsmaatregel
- Uitvoer van willekeurige code (Root/admin)
- Uitvoer van willekeurige code (Gebruiker)
- Toegang tot gevoelige gegevens

Oplossingen

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

Referenties

- <https://my.f5.com/manage/s/article/K000138757>
- <https://my.f5.com/manage/s/article/K000138932>
- <https://my.f5.com/manage/s/article/K000139656>
- <https://my.f5.com/manage/s/article/K000139778>
- <https://my.f5.com/manage/s/article/K000140578>
- <https://my.f5.com/manage/s/article/K000140920>
- <https://my.f5.com/manage/s/article/K000140933>
- <https://my.f5.com/manage/s/article/K000140947>
- <https://my.f5.com/manage/s/article/K000140950>
- <https://my.f5.com/manage/s/article/K000141003>
- <https://my.f5.com/manage/s/article/K000148587>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2014-0064	
> CVE-2014-0065	
> CVE-2014-0066	
> CVE-2014-0067	
> CVE-2019-5010	7.5 HIGH
> CVE-2019-16056	7.5 HIGH
> CVE-2022-26488	7.0 HIGH
> CVE-2024-36242	7.3 HIGH
> CVE-2024-38660	2.0 LOW
> CVE-2024-56337	7.2 HIGH
> CVE-2025-20029	8.7 HIGH
> CVE-2025-20045	8.7 HIGH
> CVE-2025-20058	8.9 HIGH
> CVE-2025-21087	8.9 HIGH
> CVE-2025-21091	8.7 HIGH
> CVE-2025-22846	8.7 HIGH
> CVE-2025-22891	8.7 HIGH
> CVE-2025-23239	8.5 HIGH
> CVE-2025-23412	8.7 HIGH
> CVE-2025-23413	6.7 MEDIUM
> CVE-2025-23415	2.3 LOW

> CVE-2025-23419	5.3 MEDIUM
> CVE-2025-24312	8.7 HIGH
> CVE-2025-24319	7.1 HIGH
> CVE-2025-24320	5.1 MEDIUM
> CVE-2025-24326	8.9 HIGH
> CVE-2025-24497	8.7 HIGH

CWE's

CWE	Beschrijving
> CWE-772	Missing Release of Resource after Effective Lifetime
> CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
> CWE-311	Missing Encryption of Sensitive Data
> CWE-426	Untrusted Search Path
> CWE-345	Insufficient Verification of Data Authenticity
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-190	Integer Overflow or Wraparound
> CWE-693	Protection Mechanism Failure
> CWE-125	Out-of-bounds Read
> CWE-401	Missing Release of Memory after Effective Lifetime
> CWE-476	NULL Pointer Dereference
> CWE-400	Uncontrolled Resource Consumption
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-787	Out-of-bounds Write
> CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

➤ CWE-20	Improper Input Validation
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

f5
big- ip
big- ip_next
big- ip_next_central_manager
big- ip_next_cnf
big- ip_next_spk
nginx_open_source
nginx_plus

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.