Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0366

Kwetsbaarheid verholpen in Fortinet FortiWeb

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-11-2025

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

Fortinet heeft een kwetsbaarheid verholpen in FortiWeb.

Duiding

Fortinet heeft een kwetsbaarheid verholpen in FortiWeb. De kwetsbaarheid met het kenmerk CVE-2025-64446 betreft een relative path traversal-kwetsbaarheid en stelt een niet-geauthenticeerde aanvaller op afstand in staat om administratieve commando's uit te voeren via speciaal vervaardigde HTTP-verzoeken.

Het NCSC heeft informatie ontvangen dat de kwetsbaarheid al enige tijd actief wordt misbruikt. Tevens hebben onderzoekers Proof-of-Concept-code (PoC) gepubliceerd waarmee de kwetsbaarheid kan worden aangetoond. Het is daarom de verwachting dat het aantal pogingen tot misbruik verder zal toenemen.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie de bijgevoegde referenties voor meer informatie.

Als het installeren van een update niet direct mogelijk is, adviseert Fortinet om HTTP en HTTPS uit te schakelen op internetgerichte interfaces. Fortinet raadt aan deze maatregel in stand te houden totdat de update kan worden uitgevoerd.

Wanneer de beheerinterface conform best practices uitsluitend intern benaderbaar is, wordt het risico aanzienlijk verminderd.

Controleer de FortiWeb-omgeving op indicatoren die door beveiligingsbedrijven zijn gedeeld. De kwetsbaarheid is namelijk al misbruikt voordat Fortinet de beveiligingsupdates uitbracht. Met name organisaties waarvan de beheerinterface via het internet toegankelijk is, lopen een verhoogd risico te zijn gecompromitteerd.

Controleer de FortiWeb-omgeving op aanwezigheid van de volgende indicatoren van beveiligingsbedrijf Qualys. Aanwezigheid kan duiden op misbruik van de kwetsbaarheid.

- Binnenkomende POST-verzoeken naar */api/v2.0/cmd/system/admin%3F/../../../../../cgi-bin/fwbcgi* of soortgelijke path-traversalpatronen afkomstig van niet-geautoriseerde IP-adressen.
- Verzoeken met base64-encoded CGINFO-headers.
- Onbekende beheerdersaccounts die sinds begin oktober 2025 zijn aangemaakt.
- Nieuwe lokale gebruikersaccounts met het toegangsprofiel prof_admin.
- Accounts met trust host-ranges ingesteld op *0.0.0.0/0* of *::/0*.

Referenties

- https://blog.qualys.com/vulnerabilities-threat-research/2025/11/14/unauthenticated-authentication-bypass-in-fortinet-fortiweb-cve-2025-64446-exploited-in-the-wild
- https://fortiguard.fortinet.com/psirt/FG-IR-25-910
- https://github.com/watchtowrlabs/watchTowr-vs-Fortiweb-AuthBypass
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-64446
- https://www.rapid7.com/blog/post/etr-critical-vulnerability-in-fortinet-fortiweb-exploited-in-the-wild

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-64446	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-23	Relative Path Traversal

Getroffen producten

Fortinet
FortiWeb
Fortiweb
Fortiweb (Application)

Disclaimer