Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0231

Kwetsbaarheden verholpen in XWiki

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2025

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

XWiki heeft kwetsbaarheden verholpen in het rendering systeem en de standaard macro content parser.

Duiding

De kwetsbaarheden in het XWiki rendering systeem stelden aanvallers in staat om XSS-aanvallen uit te voeren door de afhankelijkheid van de `xdom+xml/current` syntax. Deze kwetsbaarheid is verholpen in versie 14.10. Daarnaast waren er kwetsbaarheden in de standaard macro content parser die leidden tot privilege-escalatie en remote code execution door problemen met geneste macro's. Deze zijn gepatcht in de versies 13.10.11, 14.4.7 en 14.10. De aanvaller kon ongeautoriseerde macro's uitvoeren door de restricties in de macro content parser te omzeilen.

Oplossingen

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

Referenties

- https://github.com/xwiki/xwiki-rendering/security/advisories/GHSA-32mf-57h2-64x9
- https://github.com/xwiki/xwiki-rendering/security/advisories/GHSA-w3wh-g4m9-783p

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-53835	**5.1 MEDIUM**
CVE-2025-53836	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
CWE-94	Improper Control of Generation of Code ('Code Injection')

CWE-863	Incorrect Authorization
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

XWiki
Xwiki-rendering

Disclaimer