Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0492

Kwetsbaarheid verholpen in Apache Struts

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-12-2024
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

Additionele oplossing toegevoegd.

Feiten

Apache heeft een kwetsbaarheid verholpen in Apache Struts (Versies van 2.0.0 tot voor 6.4.0).

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop de bestandupload logica is geïmplementeerd in de verouderde **FileUploadInterceptor**. Deze kwetsbaarheid kan worden misbruikt om willekeurige code op systemen die deze versies draaien uit te voeren. Aangezien de getroffen versies veelvuldig worden gebruikt in verschillende applicaties, kan de impact aanzienlijk zijn. Applicaties die gebruik maken van het vernieuwde **ActionFileUploadInterceptor** zijn niet gevoelig voor misbruik.

Oplossingen

Apache heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Naast het inzetten van de updates moeten applicaties die gebouwd zijn met Struts aangepast worden om gebruik te maken van het nieuwe **ActionFileUploadInterceptor** in plaats van het verouderde **FileUploadInterceptor**. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://cwiki.apache.org/confluence/display/WW/S2-067
- https://struts.apache.org/core-developers/file-upload

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-53677	9.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-552	Files or Directories Accessible to External Parties

Getroffen producten

apache
struts

Disclaimer