Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0177

Kwetsbaarheden verholpen in IBM WebSphere Application Server en WebSphere Liberty

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-06-2026

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

IBM heeft kwetsbaarheden verholpen in WebSphere Application Server en WebSphere Liberty versies 8.5 en 9.0.

Duiding

De kwetsbaarheden bevinden zich in de Web Server Plug-ins die onderdeel zijn van de request handling processen van deze producten. De eerste kwetsbaarheid betreft HTTP request smuggling, waarbij speciaal opgemaakte HTTP-verzoeken worden gebruikt om beveiligingscontroles te omzeilen of de normale verwerking van HTTP-verzoeken te verstoren. De tweede kwetsbaarheid betreft remote code execution, waarbij een aanvaller door het versturen van speciaal opgemaakte verzoeken naar de plug-ins op afstand willekeurige code kan uitvoeren. Beide kwetsbaarheden richten zich op kritieke componenten die verantwoordelijk zijn voor de communicatie met de webserver binnen deze IBM-producten.

Oplossingen

IBM heeft updates uitgebracht om de kwetsbaarheden in WebSphere Application Server en WebSphere Liberty te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.ibm.com/support/pages/node/7274072
- https://www.ibm.com/support/pages/node/7274368
- https://www.ibm.com/support/pages/node/7274512
- https://www.ibm.com/support/pages/node/7274666
- https://www.ibm.com/support/pages/node/7275036

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-8620	7.5 HIGH
CVE-2026-8633	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Getroffen producten

IBM
Web Server Plug-ins for WebSphere Application Server and WebSphere Liberty
WebSphere Application Server
WebSphere Remote Server

Disclaimer