Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0078

Kwetsbaarheden verholpen in Kibana

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 05-03-2026

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

Elastic heeft kwetsbaarheden verholpen in Kibana.

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van Kibana. Een geauthenticeerde gebruiker met alleen weergaveprivileges kan een fout in de invoervalidatie misbruiken om een Denial of Service-voorwaarde te veroorzaken door speciaal vervaardigde, verkeerd gevormde payloads te verzenden. Dit leidt tot overmatig gebruik van resources en kan resulteren in crashes. Daarnaast bevat de zoekendpoint van Kibana's interne Content Connectors een kwetsbaarheid die het mogelijk maakt voor aanvallers om gemanipuleerde invoergegevens te leveren, wat ook kan leiden tot een Denial of Service. De AI Inference Anonymization Engine maakt gebruik van een inefficiënt geconstrueerde reguliere expressie, wat kan worden misbruikt om een Denial of Service te veroorzaken door de regex-processor te overweldigen. De Timelion-component kan ook worden misbruikt om ongecontroleerd middelenverbruik te veroorzaken, wat de beschikbaarheid van de Kibana-service beïnvloedt. Ten slotte staat de kwetsbaarheid in de workflow template engine geauthenticeerde gebruikers met executeWorkflow-rechten toe om code in te voegen die willekeurige bestanden van het serversysteem kan lezen en server-side request forgery (SSRF) aanvallen mogelijk maakt.

Oplossingen

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

Referenties

- https://discuss.elastic.co/t/kibana-8-19-11-9-2-5-security-update-esa-2026-14/385250
- https://discuss.elastic.co/t/kibana-8-19-11-9-2-5-security-update-esa-2026-15/385251
- https://discuss.elastic.co/t/kibana-8-19-12-9-2-6-9-3-1-security-update-esa-2026-12/385248
- https://discuss.elastic.co/t/kibana-8-19-12-9-2-6-9-3-1-security-update-esa-2026-13/385249
- https://discuss.elastic.co/t/kibana-9-3-1-security-update-esa-2026-17/385253

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-26934	6.5 MEDIUM
CVE-2026-26935	7.5 HIGH

CVE-2026-26936	7.5 HIGH
CVE-2026-26937	7.5 HIGH
CVE-2026-26938	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-400	Uncontrolled Resource Consumption
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1333	Inefficient Regular Expression Complexity
CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine

Getroffen producten

Elastic
Kibana
Open Source
Kibana

Disclaimer