



# NCSC-2026-0213

## Kwetsbaarheden verholpen in MISP platform

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 29-06-2026

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

MISP heeft meerdere kwetsbaarheden verholpen in het MISP platform.

## Duiding

De kwetsbaarheden betreffen onder andere het manipuleren van client-supplied primary en foreign keys door geauthenticeerde gebruikers, wat leidde tot ongeautoriseerd overschrijven van data, eigendomsoverdracht en wijziging van de scope van records. Verder was er een gebrekkige toegangcontrole bij bulkverwijdering van Event Reports en Sharing Groups, waardoor gebruikers met brede rolrechten items van andere organisaties konden verwijderen. Ook waren er meerdere toegangcontroleproblemen die het mogelijk maakten om ongeautoriseerde wijzigingen of verwijderingen over organisatiegrenzen heen uit te voeren. Daarnaast bevatte het platform een kwetsbaarheid waarbij geauthenticeerde sitebeheerders de NDJSON error log path konden instellen naar een webtoegankelijk PHP-bestand, wat leidde tot remote code execution via geïnjecteerde PHP-code in logbestanden. Verder konden geauthenticeerde beheerders willekeurige Kafka configuratiebestanden specificeren, waarmee arbitrary code execution mogelijk was door het laden van kwaadaardige libraries. Deze kwetsbaarheden zijn gemitigeerd door het invoeren van server-side validatie, strikte autorisatiecontroles, beperkingen op logpadconfiguraties, en het afdwingen van toegestane locaties voor configuratiebestanden.

## Oplossingen

MISP heeft updates uitgebracht waarin deze kwetsbaarheden zijn verholpen door het implementeren van server-side validatie van sleutels, per-object autorisatiecontroles bij verwijderingen, beperkingen op logpadconfiguraties, en het afdwingen van toegestane locaties voor Kafka configuratiebestanden. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://github.com/advisories/GHSA-3vhv-jx5j-gj6p>
- <https://github.com/advisories/GHSA-7v9f-64q7-x2jg>
- <https://github.com/advisories/GHSA-834x-pvxg-xh58>
- <https://github.com/advisories/GHSA-MF7V-X7R6-FQ57>
- <https://github.com/advisories/GHSA-ch28-mjgc-m4wr>
- <https://github.com/advisories/GHSA-r3v6-qw6x-wf6h>

## Kwetsbaarheden

CVE	CVSS Score
-----	------------

➤ CVE-2026-56422	9.4 CRITICAL
➤ CVE-2026-56423	9.4 CRITICAL
➤ CVE-2026-56424	7.1 HIGH
➤ CVE-2026-56425	9.3 CRITICAL
➤ CVE-2026-56446	8.7 HIGH
➤ CVE-2026-56447	9.3 CRITICAL

## CWE's

CWE	Beschrijving
➤ CWE-94	Improper Control of Generation of Code ('Code Injection')
➤ CWE-384	Session Fixation
➤ CWE-639	Authorization Bypass Through User-Controlled Key
➤ CWE-829	Inclusion of Functionality from Untrusted Control Sphere
➤ CWE-862	Missing Authorization
➤ CWE-863	Incorrect Authorization

## Getroffen producten

MISP
MISP

## Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.