



# NCSC-2025-0327

## Kwetsbaarheden verholpen in Zohocorp's ManageEngine

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 23-10-2025

**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](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

Zohocorp heeft kwetsbaarheden verholpen in ManageEngine (Specifiek voor ADManager Plus, EndPoint Central en Analytics Plus).

## Duiding

De kwetsbaarheden omvatten een geauthenticeerde command injection in ADManager Plus, XML-injecties in EndPoint Central, en een geauthenticeerde SQL-injectie in Analytics Plus. Deze kwetsbaarheden stellen aanvallers in staat om ongeautoriseerde commando's uit te voeren, toegang te krijgen tot gevoelige gegevens of de database te manipuleren. Dit kan leiden tot ernstige compromittering van systeemintegriteit en vertrouwelijkheid.

## Oplossingen

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

## Referenties

- <https://www.manageengine.com/analytics-plus/CVE-2025-9428.html>
- <https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2025-10020.html>
- <https://www.manageengine.com/products/desktop-central/parsing-xml-data.html>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-10020</a>	5.3 MEDIUM
➤ <a href="#">CVE-2025-7473</a>	4.8 MEDIUM
➤ <a href="#">CVE-2025-9428</a>	5.3 MEDIUM

## CWE's

CWE	Beschrijving
> <a href="#">CWE-77</a>	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> <a href="#">CWE-89</a>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> <a href="#">CWE-91</a>	XML Injection (aka Blind XPath Injection)

## Getroffen producten

<b>Zoho</b>
Analytics Plus
Endpoint Central
<b>Zohocorp</b>
ManageEngine ADManager Plus

## 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.