



# NCSC-2024-0458

## Kwetsbaarheden ontdekt in Veritas Enterprise Vault

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 25-11-2024

### **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

Er zijn kwetsbaarheden ontdekt in Veritas Enterprise Vault (Specifiek voor versies eerder dan 15.2).

## Duiding

De kwetsbaarheden bevinden zich in de wijze waarop Veritas Enterprise Vault omgaat met de deserialisatie van niet-vertrouwde gegevens die worden verzonden via een .NET Remoting TCP-poort. Dit stelt kwaadwillenden in staat om willekeurige code uit te voeren, wat kan leiden tot ongeautoriseerde toegang en controle over de getroffen systemen.

Voor succesvol misbruik moet de kwaadwillende rechten hebben om een RDP-verbinding op te bouwen naar een kwetsbare server. Hiervoor dient de kwaadwillende lid te zijn van de RDP-user group en kennis te hebben van de inrichting van de Veritas-infrastructuur in gebruik.

## Oplossingen

Veritas heeft (nog) geen updates uitgebracht om de kwetsbaarheden te verhelpen. Wel heeft Veritas mitigerende maatregelen gepubliceerd om het risico van misbruik weg te nemen.

- Alleen Enterprise Vault Administrators dienen toegang te hebben tot de EV server, zoals beschreven in de Enterprise Vault Administrator's Guide. (Zie: Managing Administrator Security)
- Alleen vertrouwde gebruikers mogen lid zijn van de Remote Desktop User group en mogen RDP toegang hebben tot de EV server.
- Schakel de firewall in op de EV server en configureer deze conform de informatie in de Enterprise Administrator's Guide. (Zie: Firewall Settings for Enterprise Vault programs)
- Zorg dat de laatste Windows updates zo spoedig mogelijk worden geïnstalleerd.

Veritas geeft aan de kwetsbaarheden definitief te verhelpen in Enterprise Vault 15.2. Deze wordt verwacht in het derde kwartaal van 2025.

Zie verder bijgevoegde referenties voor meer informatie.

## Referenties

➤ [https://www.veritas.com/content/support/en\\_US/security/VTS24-014](https://www.veritas.com/content/support/en_US/security/VTS24-014)

## Kwetsbaarheden

CVE	CVSS Score
<a href="#">&gt; CVE-2024-53909</a>	
<a href="#">&gt; CVE-2024-53910</a>	
<a href="#">&gt; CVE-2024-53911</a>	
<a href="#">&gt; CVE-2024-53912</a>	
<a href="#">&gt; CVE-2024-53913</a>	
<a href="#">&gt; CVE-2024-53914</a>	
<a href="#">&gt; CVE-2024-53915</a>	

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-502</a>	Deserialization of Untrusted Data

## Getroffen producten

<b>veritas</b>
enterprise_vault

## 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.