Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-53909	
CVE-2024-53910	
CVE-2024-53911	
CVE-2024-53912	
CVE-2024-53913	
CVE-2024-53914	
CVE-2024-53915	

CWE's

CWE	Beschrijving
CWE-502	Deserialization of Untrusted Data

Getroffen producten

veritas
enterprise_vault

Disclaimer