



Advisory NCSC-2026-0433

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in IBM Guardium Data Protection

Publicatiedatum: 16-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

IBM heeft meerdere kwetsbaarheden verholpen in IBM Guardium Data Protection versies 12.0, 12.1 en 12.2.

Duiding

De kwetsbaarheden betreffen onder andere remote code execution via path traversal, meerdere SQL-injectieproblemen, en diverse buffer overflow kwetsbaarheden (heap-based, stack-based en buffer overrun) in verschillende componenten zoals de MongoDB protocol parser en de TDS PRELOGIN packet decoder. Aanvallers kunnen deze kwetsbaarheden misbruiken om zonder authenticatie willekeurige code uit te voeren, toegang te krijgen tot of manipulatie uit te voeren op gevoelige data, en denial-of-service condities te veroorzaken. De kwetsbaarheden zijn aanwezig in meerdere versies van het product en kunnen leiden tot compromittering van de integriteit, vertrouwelijkheid en beschikbaarheid van de systemen waarop Guardium draait.

Oplossingen

IBM heeft updates uitgebracht om de kwetsbaarheden in Guardium Data Protection te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.ibm.com/support/pages/node/7291674>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-75875	9.8 CRITICAL
CVE-2026-80381	9.8 CRITICAL
CVE-2026-81932	8.6 HIGH
CVE-2026-82335	8.1 HIGH
CVE-2026-82895	8.1 HIGH

CVE	CVSS Score
CVE-2026-84035	8.1 HIGH
CVE-2026-84058	8.1 HIGH
CVE-2026-84198	8.1 HIGH
CVE-2026-84246	8.1 HIGH
CVE-2026-84875	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-787	Out-of-bounds Write

Getroffen producten

IBM
Guardium Data Protection

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 or 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.