



NCSC-2026-0301

Kwetsbaarheden verholpen in IBM i operating system door IBM

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-08-2026

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

IBM heeft kwetsbaarheden verholpen in IBM i operating system versies 7.3, 7.4, 7.5 en 7.6.

Duiding

De kwetsbaarheden betreffen meerdere aspecten van het IBM i - operating system, waaronder onjuist privilege management, onbeheerde zoekpadelementen, out-of-bounds reads en writes, buffer overflows (zowel heap- als stackgebaseerd), SQL-injecties, path traversal, TOCTOU-racecondities met symbolische links, onjuiste validatie van omgevingsvariabelen en profielnamen, en onjuiste neutralisatie van speciale elementen in OS-commando's. Aanvallers met geldige authenticatie kunnen deze kwetsbaarheden misbruiken om privileges te escaleren, willekeurige code uit te voeren, toegang te verkrijgen tot gevoelige gegevens, de systeemintegriteit te compromitteren of een denial-of-service te veroorzaken. De kwetsbaarheden zijn aanwezig in meerdere opeenvolgende versies van IBM i waarvoor meerdere updates zijn uitgebracht. Het advies van het NCSC is dan ook om goed te controleren of de in gebruik zijnde versie onder de kwetsbare versies valt.

Oplossingen

IBM heeft updates uitgebracht om de kwetsbaarheden in IBM i operating system versies 7.3 tot en met 7.6 te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.ibm.com/support/pages/node/7283274>
- <https://www.ibm.com/support/pages/node/7283275>
- <https://www.ibm.com/support/pages/node/7283276>
- <https://www.ibm.com/support/pages/node/7283277>
- <https://www.ibm.com/support/pages/node/7283278>
- <https://www.ibm.com/support/pages/node/7283280>
- <https://www.ibm.com/support/pages/node/7283282>
- <https://www.ibm.com/support/pages/node/7283294>
- <https://www.ibm.com/support/pages/node/7283295>
- <https://www.ibm.com/support/pages/node/7283296>
- <https://www.ibm.com/support/pages/node/7283298>
- <https://www.ibm.com/support/pages/node/7283299>
- <https://www.ibm.com/support/pages/node/7283300>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2026-16722	8.8 HIGH
> CVE-2026-16860	9.9 CRITICAL
> CVE-2026-16863	7.7 HIGH
> CVE-2026-16907	7.6 HIGH
> CVE-2026-16908	8.5 HIGH
> CVE-2026-16961	7.6 HIGH
> CVE-2026-16967	8.5 HIGH
> CVE-2026-16975	8.8 HIGH
> CVE-2026-16987	8.8 HIGH
> CVE-2026-17082	8.8 HIGH
> CVE-2026-17083	9.8 CRITICAL
> CVE-2026-17218	9.8 CRITICAL
> CVE-2026-17248	7.1 HIGH
> CVE-2026-17271	7.5 HIGH
> CVE-2026-17272	8.2 HIGH
> CVE-2026-17417	8.8 HIGH
> CVE-2026-17445	8.2 HIGH
> CVE-2026-17642	8.8 HIGH
> CVE-2026-18669	8.8 HIGH

CWE's

CWE	Beschrijving
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-73	External Control of File Name or Path
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CWE-125	Out-of-bounds Read
> CWE-250	Execution with Unnecessary Privileges
> CWE-269	Improper Privilege Management
> CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
> CWE-427	Uncontrolled Search Path Element
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-787	Out-of-bounds Write

Getroffen producten

IBM
IBM i

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.