



Advisory NCSC-2026-0431

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in IBM DataPower Gateway en on- derliggende componenten

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 beveiligingsproblemen opgelost in DataPower Gateway versies 10.5 tot 11.0 en een veelvoud aan onderliggende subcomponenten.

Duiding

De kwetsbaarheden betreffen een breed scala aan problemen zoals use-after-free bugs, race conditions, buffer overflows, null pointer dereferences, integer overflows, geheugenlekken, onjuiste validatie, en cryptografische fouten.

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die remote code execution, denial of service, cross-site scripting, en bypass van autorisatie mogelijk maken, waarbij sommige aanvallen authenticatie vereisen en andere niet.

Naast de kwetsbaarheden in DataPower Gateway heeft IBM ook een veelvoud aan kwetsbaarheden verholpen in onderliggende subcomponenten. Voor deze onderliggende subcomponenten zijn eerder updates verschenen voor de individuele systemen. IBM heeft deze updates nu verwerkt in de eigen software stack van DataPower Gateway.

Oplossingen

IBM heeft patches beschikbaar gesteld voor de DataPower Gateway-productlijn. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.ibm.com/support/pages/node/7289776>
- <https://www.ibm.com/support/pages/node/7289778>
- <https://www.ibm.com/support/pages/node/7289779>
- <https://www.ibm.com/support/pages/node/7289780>
- <https://www.ibm.com/support/pages/node/7289783>
- <https://www.ibm.com/support/pages/node/7289785>
- <https://www.ibm.com/support/pages/node/7289789>
- <https://www.ibm.com/support/pages/node/7289790>
- <https://www.ibm.com/support/pages/node/7289798>

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-53781	7.8 HIGH
CVE-2025-14087	5.6 MEDIUM
CVE-2025-14512	6.5 MEDIUM
CVE-2025-21858	8.5 HIGH
CVE-2025-22105	5.5 MEDIUM
CVE-2025-37980	5.5 MEDIUM
CVE-2025-38015	7.0 HIGH
CVE-2025-38097	7.8 HIGH
CVE-2025-38180	8.5 HIGH
CVE-2025-38400	5.5 MEDIUM
CVE-2025-38405	7.5 HIGH
CVE-2025-38441	5.5 MEDIUM
CVE-2025-38470	7.8 HIGH
CVE-2025-38653	7.8 HIGH
CVE-2025-39766	4.8 MEDIUM
CVE-2025-39797	7.8 HIGH
CVE-2025-39866	7.3 HIGH
CVE-2025-40134	7.0 HIGH
CVE-2025-48431	7.5 HIGH
CVE-2025-5278	4.4 MEDIUM
CVE-2025-68183	7.8 HIGH
CVE-2025-68211	7.0 HIGH
CVE-2025-68214	5.5 MEDIUM
CVE-2025-68347	7.8 HIGH
CVE-2025-68366	7.1 HIGH
CVE-2025-68724	7.8 HIGH
CVE-2025-71066	9.8 CRITICAL
CVE-2025-71089	7.3 HIGH

CVE	CVSS Score
CVE-2026-12143	8.7 HIGH
CVE-2026-13257	6.5 MEDIUM
CVE-2026-13258	5.4 MEDIUM
CVE-2026-13757	6.2 MEDIUM
CVE-2026-14269	9.8 CRITICAL
CVE-2026-14273	6.5 MEDIUM
CVE-2026-14496	8.2 HIGH
CVE-2026-14497	8.1 HIGH
CVE-2026-14502	9.8 CRITICAL
CVE-2026-14507	7.7 HIGH
CVE-2026-14508	6.5 MEDIUM
CVE-2026-14509	5.9 MEDIUM
CVE-2026-14888	8.1 HIGH
CVE-2026-14905	8.2 HIGH
CVE-2026-14988	6.5 MEDIUM
CVE-2026-14990	9.3 CRITICAL
CVE-2026-14991	9.8 CRITICAL
CVE-2026-14992	9.8 CRITICAL
CVE-2026-14999	7.4 HIGH
CVE-2026-15588	5.3 MEDIUM
CVE-2026-15762	9.8 CRITICAL
CVE-2026-15781	8.0 HIGH
CVE-2026-15784	8.1 HIGH
CVE-2026-15819	7.5 HIGH
CVE-2026-15822	7.5 HIGH
CVE-2026-15824	8.2 HIGH
CVE-2026-16111	7.5 HIGH
CVE-2026-16159	8.6 HIGH
CVE-2026-16161	7.5 HIGH
CVE-2026-16163	8.6 HIGH
CVE-2026-16164	7.5 HIGH

CVE	CVSS Score
CVE-2026-16165	7.5 HIGH
CVE-2026-16167	7.5 HIGH
CVE-2026-16169	7.5 HIGH
CVE-2026-16170	7.5 HIGH
CVE-2026-16176	7.5 HIGH
CVE-2026-16177	5.3 MEDIUM
CVE-2026-16178	7.5 HIGH
CVE-2026-16179	7.5 HIGH
CVE-2026-16181	7.4 HIGH
CVE-2026-16182	5.9 MEDIUM
CVE-2026-16340	9.8 CRITICAL
CVE-2026-16439	5.8 MEDIUM
CVE-2026-16440	5.7 MEDIUM
CVE-2026-16441	6.9 MEDIUM
CVE-2026-2100	7.5 HIGH
CVE-2026-22979	5.5 MEDIUM
CVE-2026-22984	8.2 HIGH
CVE-2026-22990	7.5 HIGH
CVE-2026-23002	5.5 MEDIUM
CVE-2026-23060	7.0 HIGH
CVE-2026-23110	5.5 MEDIUM
CVE-2026-23204	7.3 HIGH
CVE-2026-23209	7.3 HIGH
CVE-2026-23216	9.2 CRITICAL
CVE-2026-23243	7.8 HIGH
CVE-2026-23270	7.8 HIGH
CVE-2026-23392	7.3 HIGH
CVE-2026-23455	8.7 HIGH
CVE-2026-2391	6.3 MEDIUM
CVE-2026-31411	7.1 HIGH
CVE-2026-31419	7.3 HIGH

CVE	CVSS Score
CVE-2026-31488	7.3 HIGH
CVE-2026-31508	7.8 HIGH
CVE-2026-31532	7.3 HIGH
CVE-2026-31581	5.2 MEDIUM
CVE-2026-31607	8.7 HIGH
CVE-2026-31613	7.1 HIGH
CVE-2026-31669	7.3 HIGH
CVE-2026-31677	5.5 MEDIUM
CVE-2026-31684	7.1 HIGH
CVE-2026-31685	6.8 MEDIUM
CVE-2026-33845	9.1 CRITICAL
CVE-2026-33846	7.5 HIGH
CVE-2026-3832	3.7 LOW
CVE-2026-3833	7.4 HIGH
CVE-2026-4046	7.5 HIGH
CVE-2026-41254	7.5 HIGH
CVE-2026-41602	7.5 HIGH
CVE-2026-41606	7.5 HIGH
CVE-2026-41607	9.1 CRITICAL
CVE-2026-42009	7.5 HIGH
CVE-2026-42010	9.8 CRITICAL
CVE-2026-42011	7.4 HIGH
CVE-2026-42012	7.1 HIGH
CVE-2026-42013	8.2 HIGH
CVE-2026-42014	6.6 MEDIUM
CVE-2026-42015	5.3 MEDIUM
CVE-2026-43027	7.8 HIGH
CVE-2026-43037	9.2 CRITICAL
CVE-2026-43038	9.3 CRITICAL
CVE-2026-43056	7.8 HIGH
CVE-2026-43074	7.3 HIGH

CVE	CVSS Score
CVE-2026-43116	7.3 HIGH
CVE-2026-43125	9.2 CRITICAL
CVE-2026-43163	7.0 HIGH
CVE-2026-43190	6.3 MEDIUM
CVE-2026-43198	8.2 HIGH
CVE-2026-43260	7.8 HIGH
CVE-2026-43284	8.8 HIGH
CVE-2026-43303	7.8 HIGH
CVE-2026-43329	7.3 HIGH
CVE-2026-43499	8.5 HIGH
CVE-2026-43501	9.3 CRITICAL
CVE-2026-43868	7.5 HIGH
CVE-2026-43870	9.8 CRITICAL
CVE-2026-4437	7.5 HIGH
CVE-2026-4438	5.9 MEDIUM
CVE-2026-45852	7.3 HIGH
CVE-2026-46054	7.5 HIGH
CVE-2026-46086	7.0 HIGH
CVE-2026-46116	7.8 HIGH
CVE-2026-46173	7.8 HIGH
CVE-2026-46181	7.8 HIGH
CVE-2026-46242	7.3 HIGH
CVE-2026-46259	7.3 HIGH
CVE-2026-46300	7.8 HIGH
CVE-2026-46331	8.5 HIGH
CVE-2026-46333	7.8 HIGH
CVE-2026-46917	5.3 MEDIUM
CVE-2026-46968	5.9 MEDIUM
CVE-2026-47010	3.7 LOW
CVE-2026-47021	5.3 MEDIUM
CVE-2026-47027	5.3 MEDIUM

CVE	CVSS Score
CVE-2026-47059	3.7 LOW
CVE-2026-47063	7.5 HIGH
CVE-2026-48144	9.1 CRITICAL
CVE-2026-48145	8.2 HIGH
CVE-2026-5260	8.2 HIGH
CVE-2026-52923	7.8 HIGH
CVE-2026-52991	9.8 CRITICAL
CVE-2026-53006	8.2 HIGH
CVE-2026-53009	9.8 CRITICAL
CVE-2026-53131	6.9 MEDIUM
CVE-2026-53189	2.0 LOW
CVE-2026-53264	7.3 HIGH
CVE-2026-53266	7.3 HIGH
CVE-2026-5419	3.7 LOW
CVE-2026-5450	9.8 CRITICAL
CVE-2026-55602	6.9 MEDIUM
CVE-2026-55603	7.5 HIGH
CVE-2026-55968	8.7 HIGH
CVE-2026-55970	6.9 MEDIUM
CVE-2026-58010	8.2 HIGH
CVE-2026-58011	7.5 HIGH
CVE-2026-58012	8.2 HIGH
CVE-2026-58013	8.2 HIGH
CVE-2026-58014	8.6 HIGH
CVE-2026-58015	7.5 HIGH
CVE-2026-58016	9.1 CRITICAL
CVE-2026-58662	8.7 HIGH
CVE-2026-59879	8.7 HIGH
CVE-2026-59880	8.7 HIGH
CVE-2026-60147	6.5 MEDIUM
CVE-2026-60589	3.7 LOW

CVE	CVSS Score
CVE-2026-61308	6.8 MEDIUM
CVE-2026-63913	8.2 HIGH
CVE-2026-63952	8.4 HIGH
CVE-2026-64017	9.8 CRITICAL
CVE-2026-64530	9.8 CRITICAL
CVE-2026-64560	7.8 HIGH
CVE-2026-70906	7.5 HIGH
CVE-2026-70907	5.3 MEDIUM
CVE-2026-74581	9.8 CRITICAL
CVE-2026-82417	6.3 MEDIUM
CVE-2026-82562	6.3 MEDIUM
CVE-2026-83605	8.7 HIGH
CVE-2026-83607	8.7 HIGH
CVE-2026-83608	8.7 HIGH
CVE-2026-83613	8.7 HIGH
CVE-2026-83614	8.7 HIGH
CVE-2026-83615	8.7 HIGH
CVE-2026-83616	8.7 HIGH
CVE-2026-83619	8.7 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-91	XML Injection (aka Blind XPath Injection)

CWE	Beschrijving
CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-123	Write-what-where Condition
CWE-124	Buffer Underwrite ('Buffer Underflow')
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-131	Incorrect Calculation of Buffer Size
CWE-170	Improper Null Termination
CWE-172	Encoding Error
CWE-178	Improper Handling of Case Sensitivity
CWE-179	Incorrect Behavior Order: Early Validation
CWE-187	Partial String Comparison
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-193	Off-by-one Error
CWE-208	Observable Timing Discrepancy
CWE-248	Uncaught Exception
CWE-259	Use of Hard-coded Password
CWE-266	Incorrect Privilege Assignment
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-346	Origin Validation Error
CWE-347	Improper Verification of Cryptographic Signature
CWE-354	Improper Validation of Integrity Check Value
CWE-358	Improperly Implemented Security Check for Standard

CWE	Beschrijving
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-364	Signal Handler Race Condition
CWE-366	Race Condition within a Thread
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-390	Detection of Error Condition Without Action
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-404	Improper Resource Shutdown or Release
CWE-405	Asymmetric Resource Consumption (Amplification)
CWE-407	Inefficient Algorithmic Complexity
CWE-413	Improper Resource Locking
CWE-415	Double Free
CWE-416	Use After Free
CWE-431	Missing Handler
CWE-459	Incomplete Cleanup
CWE-475	Undefined Behavior for Input to API
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data
CWE-606	Unchecked Input for Loop Condition
CWE-611	Improper Restriction of XML External Entity Reference
CWE-617	Reachable Assertion
CWE-626	Null Byte Interaction Error (Poison Null Byte)
CWE-674	Uncontrolled Recursion
CWE-696	Incorrect Behavior Order
CWE-758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior
CWE-762	Mismatched Memory Management Routines
CWE-763	Release of Invalid Pointer or Reference
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-787	Out-of-bounds Write
CWE-789	Memory Allocation with Excessive Size Value
CWE-805	Buffer Access with Incorrect Length Value

CWE	Beschrijving
CWE-820	Missing Synchronization
CWE-821	Incorrect Synchronization
CWE-822	Untrusted Pointer Dereference
CWE-824	Access of Uninitialized Pointer
CWE-825	Expired Pointer Dereference
CWE-833	Deadlock
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-838	Inappropriate Encoding for Output Context
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-863	Incorrect Authorization
CWE-908	Use of Uninitialized Resource
CWE-909	Missing Initialization of Resource
CWE-911	Improper Update of Reference Count
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1285	Improper Validation of Specified Index, Position, or Offset in Input
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-1287	Improper Validation of Specified Type of Input
CWE-1288	Improper Validation of Consistency within Input
CWE-1333	Inefficient Regular Expression Complexity
CWE-1341	Multiple Releases of Same Resource or Handle

Getroffen producten

IBM
DataPower Gateway
DataPower Gateway 10.5.0
DataPower Gateway 10.6.0
DataPower Gateway 10.6CD
DataPower Gateway 11.0.0

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.