aDvens

Security for the greater good

Newscast

Critical vulnerability in Node.js

2024-01-23 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

Node.JS - CVE-2023-39332

On 13 October 2023, Node.js published an advisory concerning CVE-2023-39332 : a critical vulnerability that affects *Node.js*. A proof of concept was recently disclosed.

Security researcher Tobias Nießen identified an incorrect restriction of directory access when processing non-*Buffer Uint8Array* objects.

By using specially crafted requests, a remote unauthenticated attacker could achieve path traversal to bypass security restrictions.

Since 20 January 2024, a proof of concept is available in open source.

Risks

- Security bypass

Type

- *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Proof of concep

A proof of concept is available since 20 January 2024.

Affected products

- Node.js versions 18.x prior to 18.18.2
- Node.js versions 20.x prior to 20.8.1

Dependent products

- IBM Answer Retrieval for Watson Discovery 2.7.0
- IBM Business Automation Workflow Enterprise Service Bus 22.0.2
- IBM Business Automation Workflow Enterprise Service Bus 23.0.1
- IBM Business Automation Workflow traditional 19.0.0.1

- IBM Business Automation Workflow traditional 19.0.0.3
- IBM Business Automation Workflow traditional 20.0.0.1
- IBM Business Automation Workflow traditional 20.0.0.2
- IBM Business Automation Workflow traditional 21.0.1
- IBM Business Automation Workflow traditional 21.0.3.1
- IBM Business Automation Workflow traditional 22.0.1
- IBM Business Automation Workflow traditional 22.0.2
- IBM Business Automation Workflow traditional 23.0.1
- IBM Cloud Transformation Advisor 2.0.1
- IBM Cloud Transformation Advisor 3.7.1
- IBM Spectrum Control 5.4
- Fedora

Recommendations

Node JS

- Update to the latest version of *Node.js* available here.
- Additional information is available on the editor website.

IBM

- *IBM Answer Retrieval for Watson Discovery*, update to version 2.15.0 or later (Patch available here)
- *IBM Spectrum Control*, update to version 5.4.11 or later (Patch available here)
- *IBM Business Automation Workflow traditional*, apply the patch DT245355
- *IBM Business Automation Workflow Enterprise Service Bus* : apply the patch DT245355.
- Additional information for *IBM Business Automation Workflow* is available on the editor website.
- Additional information for *IBM Spectrum Control* is available on the editor website.
- Additional information for *IBM Answer Retrieval for Watson Discovery* is available on the editor website.

Fedora

- Update to the latest version of *Fedora*.
- Additional information is available on the editor website.

Sources

- https://nvd.nist.gov/vuln/detail/CVE-2023-39332
- https://security.netapp.com/advisory/ntap-20231116-0009/
- https://exchange.xforce.ibmcloud.com/vulnerabilities/268788
- https://nodejs.org/en/blog/vulnerability/october-2023-security-releases
- https://bodhi.fedoraproject.org/updates/FEDORA-2023-4d2fd884ea
- https://www.ibm.com/support/pages/node/7087510?_ga=2.199109674.424467990.1705926133-1391590523.1663137482
- https://www.ibm.com/support/pages/node/7108595?_ga=2.199109674.424467990.1705926133-1391590523.1663137482
- https://www.ibm.com/support/pages/node/7109016?_ga=2.199803307.424467990.1705926133-1391590523.1663137482