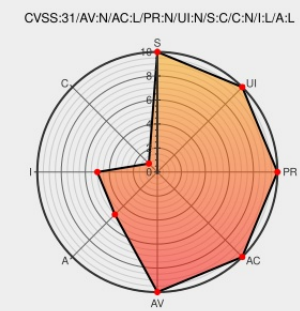
CVE-2023-26919

Published on: Not Yet Published

Last Modified on: 04/14/2023 05:03:00 PM UTC

CVE-2023-26919

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nashorn Sandbox from Javadelight contain the following vulnerability:

delight-nashorn-sandbox 0.2.4 and 0.2.5 is vulnerable to sandbox escape. When allowExitFunctions is set to false, the loadWithNewGlobal function can be used to invoke the exit and quit methods to exit the Java process.

CVE-2023-26919 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	LOW	LOW

CVE References

Description	Tags	Link
When allowExitFunctions is set to false, we can use the loadWithNewGlobal function to invoke the exit and quit methods to exit the Java process. · Issue #135 · javadelight/delight-nashorn-sandbox · GitHub	Exploit, Issue Tracking, Vendor Advisory, github.com, text/html	MISC github.com/javadelight/delight-nashorn-sandbox/issues/135

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Javadelight	Nashorn Sandbox	0.2.4	All	All	All
Application	Javadelight	Nashorn Sandbox	0.2.5	All	All	All

cpe:2.3:a:javadelight:nashorn_sandbox:0.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:javadelight:nashorn_sandbox:0.2.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-26919 : delight-nashorn-sandbox 0.2.4 and 0.2.5 is vulnerable to sandbox escape. When allowExitFunctions i… twitter.com/i/web/status/1…	2023-04-10 16:03:37
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-26919 delight-nashorn-sandbox 0.2.4 and 0.2.5 is vulnerable to sandbox… twitter.com/i/web/status/1…	2023-04-10 17:11:05

← Previous ID

Next ID→