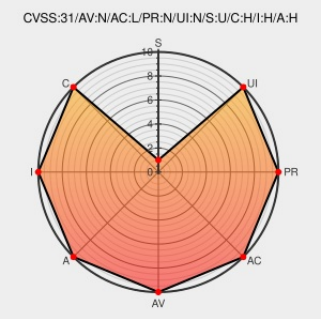
CVE-2023-22496

Published on: Not Yet Published

Last Modified on: 01/24/2023 06:52:00 PM UTC

CVE-2023-22496 - advisory for GHSA-xg38-3vmw-2978

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



Certain versions of Netdata from Netdata contain the following vulnerability:

Netdata is an open source option for real-time infrastructure monitoring and troubleshooting. An attacker with the ability to establish a streaming connection can execute arbitrary commands on the targeted Netdata agent. When an alert is triggered, the function `health_alarm_execute` is called. This function performs different checks and then enqueues a command by calling `spawn_enq_cmd`. This command is populated with several arguments that are not sanitized. One of them is the `registry_hostname` of the node for which the alert is raised. By providing a specially crafted `registry_hostname` as part of the health data that is streamed to a Netdata (parent) agent, an attacker can execute arbitrary commands at the remote host as a side-effect of the raised alert. Note that the commands are executed as the user running the Netdata Agent. This user is usually named `netdata`. The ability to run arbitrary commands may allow an attacker to escalate privileges by escalating other vulnerabilities in the system, as that user. The problem has been fixed in: Netdata agent v1.37 (stable) and Netdata agent v1.36.0-409 (nightly). As a workaround, streaming is not enabled by default. If you have previously enabled this, it can be disabled. Limiting access to the port on the recipient Agent to trusted child connections may mitigate the impact of this vulnerability.

CVE-2023-22496 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **netdata** - **netdata** version **= < 1.36.0-409**

Affected Vendor/Software: **netdata** - **netdata** version **= < 1.37**

CVSS3 Score: 9.8 - CRITICAL

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

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Netdata Streaming Alert Command Injection · Advisory · netdata/netdata · GitHub	github.com text/html	MISC github.com/netdata/netdata/security/advisories/GHSA-xg38-3vmw-2978

Related QID Numbers

182147 Debian Security Update for netdata (CVE-2023-22496)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netdata	Netdata	All	All	All	All

cpe:2.3:a:netdata:netdata:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-22496 : Netdata is an open source option for real-time infrastructure monitoring and troubleshooting. An a… twitter.com/i/web/status/1…	2023-01-14 01:07:34

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report