



CVE-2023-22497

Published on: Not Yet Published

Last Modified on: 01/24/2023 05:35:00 PM UTC

CVE-2023-22497 - advisory for GHSA-jx85-39cw-66f2

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Netdata](#) from [Netdata](#) contain the following vulnerability:

Netdata is an open source option for real-time infrastructure monitoring and troubleshooting. Each Netdata Agent has an automatically generated MACHINE GUID. It is generated when the agent first starts and it is saved to disk, so that it will persist across restarts and reboots.

Anyone who has access to a Netdata Agent has access to its

MACHINE_GUID. Streaming is a feature that allows a Netdata Agent to act as parent for other Netdata Agents (children), offloading children from various functions (increased data retention, ML, health monitoring, etc) that can now be handled by the parent Agent. Configuration is done via `stream.conf`. On the parent side, users configure in `stream.conf` an API key (any random UUID can do) to provide common configuration for all children using this API key and per MACHINE GUID configuration to customize the configuration for each child. The way this was implemented, allowed an attacker to use a valid MACHINE_GUID as an API key. This affects all users who expose their Netdata Agents (children) to non-trusted users and they also expose to the same users Netdata Agent parents that aggregate data from all these children. The problem has been fixed in: Netdata agent v1.37 (stable) and Netdata agent v1.36.0-409 (nightly). As a workaround, do not enable streaming 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-2023-22497 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: **9.1 - CRITICAL**

Attack
Vector

NETWORK

Attack
Complexity

LOW

Privileges
Required

NONE

User
Interaction

NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE

CVE References

Description	Tags	Link
Netdata Streaming Authentication Bypass · Advisory · netdata/netdata · GitHub	github.com text/html	MISC github.com/netdata/netdata/security/advisories/GHSA-jx85-39cw-66f2
Release v1.37.0 · netdata/netdata · GitHub	github.com text/html	MISC github.com/netdata/netdata/releases/tag/v1.37.0

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

183738 Debian Security Update for netdata (CVE-2023-22497)

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-2023-22497 : Netdata is an open source option for real-time infrastructure monitoring and troubleshooting. Each... twitter.com/i/web/status/1...	2023-01-14 02:07:11

[← Previous ID](#)
[Next ID →](#)

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)