



CVE-2023-34969

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-34969
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-08 03:15:00 UTC
Updated	2023-11-15 03:26:00 UTC
Description	D-Bus before 1.15.6 sometimes allows unprivileged users to crash dbus-daemon. If a privileged user with control over the c

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	D-bus Project	D-bus	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All

References

Reference
[SECURITY] Fedora 38 Update: mingw-dbus-1.14.8-1.fc38 - package-announce - Fedora Mailing-Lists
CVE-2023-xxxx: dbus-daemon crashes when a monitor is active and a message from the driver cannot be delivered (#457) · Issues · dbus / c
[SECURITY] [DLA 3628-1] dbus security update
[SECURITY] Fedora 38 Update: mingw-dbus-1.14.8-1.fc38 - package-announce - Fedora Mailing-Lists
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160843](#) Oracle Enterprise Linux Security Update for dbus (ELSA-2023-4498)

160860 Oracle Enterprise Linux Security Update for dbus (ELSA-2023-4569)
199750 Ubuntu Security Notification for DBus Vulnerability (USN-6372-1)
241917 Red Hat Update for dbus (RHSA-2023:4498)
241933 Red Hat Update for dbus (RHSA-2023:4569)
242045 Red Hat Update for dbus (RHSA-2023:5193)
284055 Fedora Security Update for mingw (FEDORA-2023-d22162d9ba)
355463 Amazon Linux Security Advisory for dbus : ALAS2023-2023-213
357026 Amazon Linux Security Advisory for dbus : ALAS2-2024-2428
378773 Alibaba Cloud Linux Security Update for dbus (ALINUX3-SA-2023:0092)
6000277 Debian Security Update for dbus (DLA 3628-1)
6140276 AWS Bottlerocket Security Update for libdbus (GHSA-4hc7-qjp6-4f9m)
673263 EulerOS Security Update for dbus (EulerOS-SA-2023-2609)
673295 EulerOS Security Update for dbus (EulerOS-SA-2023-2579)
673383 EulerOS Security Update for dbus (EulerOS-SA-2023-2807)
673518 EulerOS Security Update for dbus (EulerOS-SA-2023-2840)
673707 EulerOS Security Update for dbus (EulerOS-SA-2023-2857)
673760 EulerOS Security Update for dbus (EulerOS-SA-2023-2783)
674051 EulerOS Security Update for dbus (EulerOS-SA-2023-3122)
754190 SUSE Enterprise Linux Security Update for dbus-1 (SUSE-SU-2023:2879-1)
754191 SUSE Enterprise Linux Security Update for dbus-1 (SUSE-SU-2023:2876-1)
907735 Common Base Linux Mariner (CBL-Mariner) Security Update for dbus (27178-1)
941210 AlmaLinux Security Update for dbus (ALSA-2023:4498)
941216 AlmaLinux Security Update for dbus (ALSA-2023:4569)

© CVE.report 2026 |

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](#).

Free CVE JSON API cve.report/api

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