CVE-2021-3560

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3560
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-16 19:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	It was found that polkit could be tricked into bypassing the credential checks for D-Bus requests, elevating the privileges of

Risk And Classification

EPSS: 0.109120000 probability, percentile 0.933620000 (date 2026-04-01)

CISA KEV: Listed on 2023-05-12; due 2023-06-02; ransomware use Unknown

Problem Types: CWE-754

CISA Known Exploited Vulnerability

Vendor	Red Hat
Product	Polkit
Name	Red Hat Polkit Incorrect Authorization Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://bugzilla.redhat.com/show_bug.cgi?id=1961710; https://nvd.nist.gov/vuln/detail/CVE-2021-3560

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Polkit Project	Polkit	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Openshift Container Platform	4.7	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

. .

References

Reference	Source
Facebook Fizz Denial Of Service ≈ Packet Storm	
polkit Authentication Bypass ≈ Packet Storm	MISC
1961710 – (CVE-2021-3560) CVE-2021-3560 polkit: local privilege escalation using polkit_system_bus_name_get_creds_sync()	MISC
Privilege escalation with polkit: How to get root on Linux with a seven-year-old bug | The GitHub Blog	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159244 Oracle Enterprise Linux Security Update for polkit (ELSA-2021-2238)
- 179889 Debian Security Update for policykit-1 (CVE-2021-3560)
- 198399 Ubuntu Security Notification for polkit vulnerability (USN-4980-1)
- 239363 Red Hat Update for polkit (RHSA-2021:2238)
- 239364 Red Hat Update for polkit (RHSA-2021:2237)
- 239365 Red Hat Update for polkit (RHSA-2021:2236)
- 239490 Red Hat Update for OpenShift Container Platform 4.7.19 (RHSA-2021:2555)
- 281486 Fedora Security Update for polkit (FEDORA-2021-0ec5a8a74b)
- 281706 Fedora Security Update for polkit (FEDORA-2021-3f8d6016c9)
- 296053 Oracle Solaris 11.4 Support Repository Update (SRU) 35.94.4 Missing (CPUJUL2021)
- 376987 Alibaba Cloud Linux Security Update for polkit (ALINUX3-SA-2021:0035)
- 501899 Alpine Linux Security Update for polkit
- 670553 EulerOS Security Update for polkit (EulerOS-SA-2021-2311)
- 670779 EulerOS Security Update for polkit (EulerOS-SA-2021-2537)
- 670803 EulerOS Security Update for polkit (EulerOS-SA-2021-2561)
- 690112 Free Berkeley Software Distribution (FreeBSD) Security Update for polkit (36a35d83-c560-11eb-84ab-e0d55e2a8bf9)
- 710037 Gentoo Linux polkit Privilege escalation (GLSA 202107-31)

750102 SUSE Enterprise Linux Security Update for polkit (SUSE-SU-2021:1844-1)

750103 SUSE Enterprise Linux Security Update for polkit (SUSE-SU-2021:1842-1)

750104 SUSE Enterprise Linux Security Update for polkit (SUSE-SU-2021:1843-1)

750173 OpenSUSE Security Update for polkit (openSUSE-SU-2021:0838-1)

750763 OpenSUSE Security Update for polkit (openSUSE-SU-2021:1843-1)

770072 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021:2555)

770103 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-2555)

900684 Common Base Linux Mariner (CBL-Mariner) Security Update for polkit (8686)

940425 AlmaLinux Security Update for polkit (ALSA-2021:2238)

960004 Rocky Linux Security Update for polkit (RLSA-2021:2238)