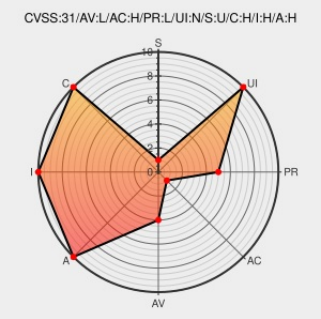
CVE-2021-3864

Published on: Not Yet Published

Last Modified on: 02/12/2023 11:42:00 PM UTC

CVE-2021-3864

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

A flaw was found in the way the dumpable flag setting was handled when certain SUID binaries executed its descendants. The prerequisite is a SUID binary that sets real UID equal to effective UID, and real GID equal to effective GID. The descendant will then have a dumpable value set to 1. As a result, if the descendant process crashes and core_pattern is set to a relative value, its core dump is stored in the current directory with uid:gid permissions. An unprivileged local user with eligible root SUID binary could use this flaw to place core dumps into root-owned directories, potentially resulting in escalation of privileges.

CVE-2021-3864 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
2015046 – (CVE-2021-3864) CVE-2021-3864 kernel: descendant's dumpable setting with certain SUID binaries	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2015046
Re: [PATCH] exec: Make suid_dumpable apply to SUID/SGID binaries irrespective of invoking users - Willy Tarreau	lore.kernel.org text/html	MISC lore.kernel.org/all/20211226150310.GA992@1wt.eu/
oss-security - Core-dump handing issues with suid	www.openwall.com	MISC www.openwall.com/lists/oss-

binaries	text/html	security/2021/10/20/2
[PATCH RFC v2 0/4] coredump: mitigate privilege escalation of process coredump - Wander Lairson Costa	lore.kernel.org text/html	MISC lore.kernel.org/lkml/20211228170910.623156-1-wander@redhat.com/
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2021-3864
CVE-2021-3864	security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2021-3864
[PATCH] exec: Make suid_dumpable apply to SUID/SGID binaries irrespective of invoking users - Waiman Long	lore.kernel.org text/html	MISC lore.kernel.org/all/20211221021744.864115-1-longman@redhat.com/

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@elordcs	@lordteruki @h4x0r_dz As stupid and simple as the Microsoft Azure Linux OMI LPE vulnerability (CVE-2021-3864[5/8/9]… twitter.com/i/web/status/1…	2021-10-06 20:50:06
@CVEreport	CVE-2021-3864 : A flaw was found in the way the dumpable flag setting was handled when certain SUID binaries execut… twitter.com/i/web/status/1…	2022-08-26 16:08:24
@vuldb	[Vuln] The severity is increased for this new vulnerability affecting Linux Kernel (CVE-2021-3864) vuldb.com/?id.207384	2022-08-26 18:59:47
@vuldb	[CTI] Some increased actor activities are shown targeting Linux Kernel (CVE-2021-3864) vuldb.com/?ctiid.207384	2022-08-27 17:29:40
/r/netcve	CVE-2021-3864	2022-08-26 17:13:08

← 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 registred 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