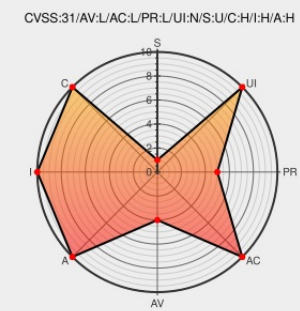
CVE-2022-30688

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2022-30688

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



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

needrestart 0.8 through 3.5 before 3.6 is prone to local privilege escalation. Regexes to detect the Perl, Python, and Ruby interpreters are not anchored, allowing a local user to escalate privileges when needrestart tries to detect if interpreters are using old source files.

CVE-2022-30688 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 3013-1] needrestart security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20220518 [SECURITY] [DLA 3013-1] needrestart security update
oss-security - CVE-2022-30688: needrestart 0.8+ local	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2022/05/17/9

privilege escalation		
[Interp] CVE-2022-30688: Anchor interpreter regex to prevent local pr… · liske/needrestart@e6e5813 · GitHub	github.com text/html	MISC github.com/liske/needrestart/commit/e6e58136e1e3c92296e2e810cb8372a5fe0dbd30
[SECURITY] [DSA 5137-1] needrestart security update	lists.debian.org text/html	MISC lists.debian.org/debian-security-announce/2022/msg00105.html
oss-security - CVE-2022-30688: needrestart 0.8+ local privilege escalation	www.openwall.com text/html	MLIST [oss-security] 20220517 CVE-2022-30688: needrestart 0.8+ local privilege escalation
Release v3.6 · liske/needrestart · GitHub	github.com text/html	MISC github.com/liske/needrestart/releases/tag/v3.6
Debian -- Security Information -- DSA-5137-1 needrestart	www.debian.org Depreciated Link text/html	DEBIAN DSA-5137

Related QID Numbers

179295 Debian Security Update for needrestart (DLA 3013-1)

179297 Debian Security Update for needrestart (DSA 5137-1)

183191 Debian Security Update for needrestart (CVE-2022-30688)

198792 Ubuntu Security Notification for needrestart Vulnerability (USN-5426-1)

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	Debian	Debian Linux	9.0	All	All	All
Application	Needrestart Project	Needrestart	All	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:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:needrestart_project:needrestart:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-30688 : needrestart 0.8 through 3.5 before 3.6 is prone to local privilege escalation. Regexes to detect t… twitter.com/i/web/status/1…	2022-05-17 19:05:43
@LinInfoSec	Debian - CVE-2022-30688: openwall.com/lists/oss-secu…	2022-05-17 21:02:08
/r/netcve	CVE-2022-30688	2022-05-17 20:38:56

← Previous ID

Next ID→