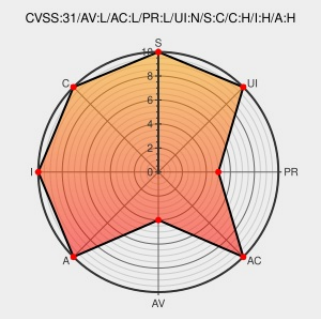
CVE-2020-29040

Published on: 11/24/2020 12:00:00 AM UTC

Last Modified on: 04/26/2022 04:34:00 PM UTC

CVE-2020-29040

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



Certain versions of Xen from Xen contain the following vulnerability:

An issue was discovered in Xen through 4.14.x allowing x86 HVM guest OS users to cause a denial of service (stack corruption), cause a data leak, or possibly gain privileges because of an off-by-one error. NOTE: this issue is caused by an incorrect fix for CVE-2020-27671.

CVE-2020-29040 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	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
XSA-355 - Xen Security Advisories	xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-355.html
oss-security - Xen Security Advisory 355 v3 (CVE-2020-29040) - stack corruption from XSA-346 change	www.openwall.com text/html	MLIST [oss-security] 20210119 Xen Security Advisory 355 v3 (CVE-2020-29040) - stack corruption from XSA-346

		change
XSA-355 - Xen Security Advisories	Vendor Advisory xenbits.xen.org text/html	MISC xenbits.xen.org/xsa/advisory-355.html

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

377780 Citrix XenServer Security Updates (CTX286511)

500795 Alpine Linux Security Update for xen

501514 Alpine Linux Security Update for xen

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	All	All	All	All

cpe:2.3:o:xen:xen:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Xen - CVE-2020-29040: xenbits.xen.org/xsa/advisory-3…	2022-04-26 19:07:00

← Previous ID

Next ID→

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