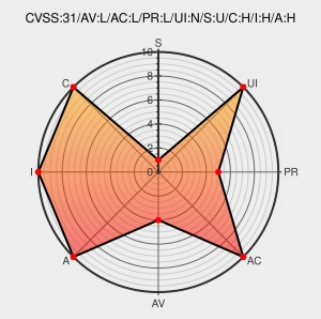
CVE-2022-31676

Published on: Not Yet Published

Last Modified on: 11/16/2022 08:05:00 PM UTC

CVE-2022-31676

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



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

VMware Tools (12.0.0, 11.x.y and 10.x.y) contains a local privilege escalation vulnerability. A malicious actor with local non-administrative access to the Guest OS can escalate privileges as a root user in the virtual machine.

CVE-2022-31676 has been assigned by security@vmware.com 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

CVE References

Description	Tags	Link
[SECURITY] Fedora 37 Update: open-vm-tools-12.1.0-1.fc37 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-1b8d3b2845
open-vm-tools: Local Privilege Escalation (GLSA 202210-27) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202210-27
oss-security - [SECURITY ADVISORY] open-vm-tools: Local privilege escalation vulnerability (CVE-2022-31676)	www.openwall.com text/html	MLIST [oss-security] 20220823 [SECURITY ADVISORY] open-vm-tools: Local privilege escalation vulnerability (CVE-2022-31676)
[SECURITY] Fedora 35 Update: open-vm-tools-12.1.0-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-1c9c0bacaf
[SECURITY] Fedora 36 Update: open-vm-tools-12.0.5-3.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-cd23eac6f4
Debian -- Security Information -- DSA-5215-1 open-vm-	www.debian.org	DEBIAN DSA-5215

tools	Depreciated Link text/html	
[SECURITY] [DLA 3081-1] open-vm-tools security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20220825 [SECURITY] [DLA 3081-1] open-vm-tools security update
CVE-2022-31676 VMware Tools Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20221017-0003/
VMSA-2022-0024	www.vmware.com text/html	MISC www.vmware.com/security/advisories/VMSA-2022-0024.html

Related QID Numbers

160075 Oracle Enterprise Linux Security Update for open-vm-tools (ELSA-2022-6357)

160079 Oracle Enterprise Linux Security Update for open-vm-tools (ELSA-2022-6358)

160080 Oracle Enterprise Linux Security Update for open-vm-tools (ELSA-2022-6381)

180961 Debian Security Update for open-vm-tools (DSA 5215-1)

180964 Debian Security Update for open-vm-tools (DLA 3081-1)

184492 Debian Security Update for open-vm-tools (CVE-2022-31676)

198908 Ubuntu Security Notification for Open VM Tools Vulnerability (USN-5578-1)

240650 Red Hat Update for open-vm-tools (RHSA-2022:6358)

240651 Red Hat Update for open-vm-tools (RHSA-2022:6356)

240652 Red Hat Update for open-vm-tools (RHSA-2022:6355)

240653 Red Hat Update for open-vm-tools (RHSA-2022:6357)

240654 Red Hat Update for open-vm-tools (RHSA-2022:6381)

257194 CentOS Security Update for open-vm-tools (CESA-2022:6381)

283095 Fedora Security Update for open (FEDORA-2022-cd23eac6f4)

283124 Fedora Security Update for open (FEDORA-2022-1c9c0bacaf)

355593 Amazon Linux Security Advisory for open-vm-tools : ALAS2-2023-2114

376866 VMware Tools Local Privilege Escalation Vulnerability (VMSA-2022-0024)

377054 Alibaba Cloud Linux Security Update for open-vm-tools (ALINUX2-SA-2022:0039)

377104 Alibaba Cloud Linux Security Update for open-vm-tools (ALINUX3-SA-2022:0159)

502492 Alpine Linux Security Update for open-vm-tools

502493 Alpine Linux Security Update for open-vm-tools

502494 Alpine Linux Security Update for open-vm-tools

710657 Gentoo Linux open-vm-tools Local Privilege Escalation Vulnerability (GLSA 202210-27)

752518 SUSE Enterprise Linux Security Update for open-vm-tools (SUSE-SU-2022:2935-1)

752519 SUSE Enterprise Linux Security Update for open-vm-tools (SUSE-SU-2022:2936-1)

752527 SUSE Enterprise Linux Security Update for open-vm-tools (SUSE-SU-2022:2961-1)

752531 SUSE Enterprise Linux Security Update for open-vm-tools (SUSE-SU-2022:2985-1)

752537 SUSE Enterprise Linux Security Update for open-vm-tools (SUSE-SU-2022:2986-1)

940656 AlmaLinux Security Update for open-vm-tools (ALSA-2022:6357)

940658 AlmaLinux Security Update for open-vm-tools (ALSA-2022:6358)

960382 Rocky Linux Security Update for open-vm-tools (RLSA-2022:6357)

960483 Rocky Linux Security Update for open-vm-tools (RLSA-2022:6358)

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	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Vmware	Tools	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:fedoraproject:fedora:36:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:37:*:*:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:tools:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@DavidCSloane	Vmware Tools for Windows and Linux local privilege escalation CVSSv3 7.0 CVE-2022-31676 twitter.com/VMwareSRC/stat…	2022-08-23 16:46:54
@sammargh	CVE-2022-31676 was posted recently and if you are a VMware shop just a heads up that it's a nasty one. All guests n… twitter.com/i/web/status/1…	2022-08-23 19:50:47
@CVEreport	CVE-2022-31676 : VMware Tools 12.0.0, 11.x.y and 10.x.y contains a local privilege escalation vulnerability. A ma… twitter.com/i/web/status/1…	2022-08-23 20:10:09
@wdormann	Hints to what the recently-patched CVE-2022-31676 LPE in VMware *guests* where VMware tools are installed are in th… twitter.com/i/web/status/1…	2022-08-23 20:37:53
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-31676 - VMware Tools (12.0.0, 11.x.y and 10.x.y) contains a local privilege e… twitter.com/i/web/status/1…	2022-08-23 20:42:15
@0xF21D	VMware tools allows for priv escalation, CVE-2022-31676: vmware.com/security/advis… Looks like it is improperly autho… twitter.com/i/web/status/1…	2022-08-23 20:58:10
@oss_security	[SECURITY ADVISORY] open-vm-tools: Local privilege escalation vulnerability (CVE-2022-31676): Posted by VMware Secu… twitter.com/i/web/status/1…	2022-08-24 01:30:14
@autumn_good_35	合わせ技で使われそうですね。 VMware Tools update addresses a local privilege escalation vulnerability (CVE-2022-31676)… twitter.com/i/web/status/1…	2022-08-24 02:38:26
@sidfm_jp	VMware Tools にゲストシステムの root 権限を奪われる問題 (CVE-2022-31676) [43146] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2022-08-24 04:30:03
@ohhara_shiojiri	"The vulnerability, tracked as CVE-2022-31676, could be exploited by attackers to escalate privileges on a compromised system."	2022-08-24 05:06:19
@Regnor	Please also be aware that open-vm-tools are affected by VMSA-2022-0024 / CVE-2022-31676. #VMware github.com/vmware/open-vm…	2022-08-24 06:50:36
@vuldb	[Vuln] There is a new vulnerability with elevated criticality in VMware Tools (CVE-2022-31676) vuldb.com/?id.207051	2022-08-24 06:57:49
@siskrn	VMware Toolsの脆弱性 CVE-2022-31676 、open-vm-tools(Linux Distributionに入っているもの)にもあるのか？	2022-08-24 07:01:51
@autumn_good_35	公開タイミング的にCVE-2022-31676のことかと思いますが、この内容だとゲストOSの権限昇格ではなくて、外部からの認証回避だと誤解されそうです? 大阪府警本部 サイバーセキュリティ対策通信（VMware製品に脆弱性！）… twitter.com/i/web/status/1…	2022-08-24 08:32:54
@__kokumoto	VMWareがVMWare Toolsにおける権限昇格の脆弱性(CVE-2022-31676)を修正。ゲストOSの非特権アクセスを用いて、仮想マシンのrootに昇格可能。WindowsとLinux双方に影響。 VMWare Tool… twitter.com/i/web/status/1…	2022-08-24 11:33:36
@andresbohren	#VMware has released #VMwareTools 12.1.0 to fix the Issues in CVE-2022-31676 bit.ly/3KjckHt https://t.co/xhMRL9RkNE	2022-08-24 13:35:10
@Har_sia	CVE-2022-31676 har-sia.info/CVE-2022-31676… #HarsiaInfo	2022-08-24 15:01:08
@Monitoring_IT	VMware Tools update 12.1.0 to fix CVE-2022-31676 buff.ly/3pNDCMt	2022-08-24 16:51:08
@vuldb	[CTI] A lot of offensive activities were identified targeting VMware Tools (CVE-2022-31676) vuldb.com/?ctiid.207051	2022-08-24 18:27:18
@cyberkendra	(CVE-2022-31676) Local privilege escalation vulnerability vmware.com/security/advis… #security #VMware	2022-08-24 19:48:27

@omokazuki	SIOSセキュリティブログを更新しました。 VMWare Tools(open-vm-tools)の脆弱性(Important: CVE-2022-31676) #sios_tech #security… twitter.com/i/web/status/1…	2022-08-25 00:55:31
@itit7777	VMWare Tools(open-vm-tools)の脆弱性(Important: CVE-2022-31676) security.sios.com/vulnerability/…	2022-08-25 01:15:05
@dnsmichi	#hugops CVE-2022-31676 VMware Tools (12.0.0, 11.x.y and 10.x.y) contains a local privilege escalation vulnerabilit… twitter.com/i/web/status/1…	2022-08-25 08:03:18
@jbhall56	An insider threat or remote attacker with initial access could exploit CVE-2022-31676 to steal sensitive data and s… twitter.com/i/web/status/1…	2022-08-25 10:22:41
@Runecast	Concerned about CVE-2022-31676 #vulnerability? Don't worry, Runecast already has you covered and automatically dete… twitter.com/i/web/status/1…	2022-08-25 12:29:59
@Har_sia	CVE-2022-31676 har-sia.info/CVE-2022-31676… #HarsiaInfo	2022-08-25 15:01:08
@securezoo	VMware Tools update fixes local privilege escalation vulnerability (CVE-2022-31676) buff.ly/3PPm8tU… twitter.com/i/web/status/1…	2022-08-25 16:00:35
@vspinmaster	Heads up, VMware released VMSA-2022-0024 related to a new CVE-2022-31676 in VMware Tools. If you are wondering how… twitter.com/i/web/status/1…	2022-08-25 20:36:05
@siskrn	RHELはAffectedで対応待ち access.redhat.com/security/cve/C…	2022-08-26 03:44:14
@Esben_Dochy	VMware released a VMware Tools security update to fix CVE-2022-31676, a local privilege escalation vulnerability. B… twitter.com/i/web/status/1…	2022-08-26 14:20:16
@ispcolohost	@RedHat every other vendor has patches out for access.redhat.com/security/cve/c… any updates?	2022-08-27 09:24:39
@JonathanHCare	If its not local, it's just fizzy hacks. "The vulnerability, tracked as CVE-2022-31676, could be exploited by attac… twitter.com/i/web/status/1…	2022-08-27 10:06:01
/r/cybersecurity	VMware Tools update addresses a local privilege escalation vulnerability (CVE-2022-31676) with a maximum CVSSv3 base score of 7.0	2022-08-23 17:26:18
/r/vmware	VMware Tools update addresses a local privilege escalation vulnerability (CVE-2022-31676) with a maximum CVSSv3 base score of 7.0	2022-08-23 17:23:18
/r/netcve	CVE-2022-31676	2022-08-23 21:38:28
/r/CentOS	Security update of the Open-vm-tools package	2022-09-05 08:42:15
/r/RockyLinux	Open-vm-tools v12.1.0	2022-09-21 08:43:44
/r/vmware	Virtual machine marked invalid after vmware tools upgrade 12.1.0 on ESXi 6.5 EP26	2022-11-16 11:48:44
/r/crowdstrike	How long for a vulnerability to clear and how to check the new "scan" is "current" ?	2023-01-03 16:36:42

← Previous ID

Next ID→

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