



CVE-2022-33912

Published on: Not Yet Published

Last Modified on: 06/28/2022 02:39:00 PM UTC

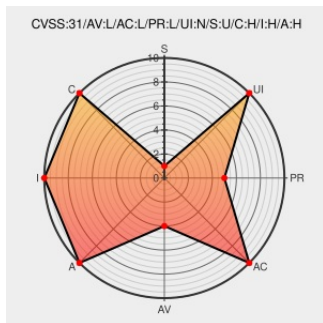
CVE-2022-33912

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Checkmk](#) from [Tribe29](#) contain the following vulnerability:

A permission issue affects users that deployed the shipped version of the Checkmk Debian package. Packages created by the agent bakery (enterprise editions only) were not affected. Using the shipped version of the agents, the maintainer scripts located at `/var/lib/dpkg/info/` will be owned by the user and the group with ID 1001. If such a user exists on the system, they can change the content of these files (which are then executed by root). This leads to a local privilege escalation on the monitored host. Version 1.6 through 1.6.9p29, version 2.0 through 2.0.0p26, version 2.1 through 2.1.0p3, and version 2.2.0i1 are affected.

CVE-2022-33912 has been assigned by [M](#) 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: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
-------------	------	------

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tribe29	Checkmk	1.6.0	-	All	All
Application	Tribe29	Checkmk	1.6.0	b1	All	All
Application	Tribe29	Checkmk	1.6.0	b10	All	All
Application	Tribe29	Checkmk	1.6.0	b12	All	All
Application	Tribe29	Checkmk	1.6.0	b3	All	All
Application	Tribe29	Checkmk	1.6.0	b4	All	All
Application	Tribe29	Checkmk	1.6.0	b5	All	All
Application	Tribe29	Checkmk	1.6.0	b9	All	All
Application	Tribe29	Checkmk	1.6.0	p1	All	All
Application	Tribe29	Checkmk	1.6.0	p10	All	All
Application	Tribe29	Checkmk	1.6.0	p11	All	All
Application	Tribe29	Checkmk	1.6.0	p12	All	All
Application	Tribe29	Checkmk	1.6.0	p13	All	All
Application	Tribe29	Checkmk	1.6.0	p14	All	All
Application	Tribe29	Checkmk	1.6.0	p15	All	All
Application	Tribe29	Checkmk	1.6.0	p16	All	All
Application	Tribe29	Checkmk	1.6.0	p19	All	All
Application	Tribe29	Checkmk	1.6.0	p2	All	All
Application	Tribe29	Checkmk	1.6.0	p20	All	All
Application	Tribe29	Checkmk	1.6.0	p21	All	All
Application	Tribe29	Checkmk	1.6.0	p22	All	All
Application	Tribe29	Checkmk	1.6.0	p23	All	All
Application	Tribe29	Checkmk	1.6.0	p24	All	All
Application	Tribe29	Checkmk	1.6.0	p25	All	All
Application	Tribe29	Checkmk	1.6.0	p26	All	All
Application	Tribe29	Checkmk	1.6.0	p27	All	All

Application	Tribe29	Checkmk	1.6.0	p28	All	All
Application	Tribe29	Checkmk	1.6.0	p29	All	All
Application	Tribe29	Checkmk	1.6.0b10	All	All	All
Application	Tribe29	Checkmk	1.6.0b11	All	All	All
Application	Tribe29	Checkmk	2.0.0	-	All	All
Application	Tribe29	Checkmk	2.0.0	b1	All	All
Application	Tribe29	Checkmk	2.0.0	b2	All	All
Application	Tribe29	Checkmk	2.0.0	b3	All	All
Application	Tribe29	Checkmk	2.0.0	b4	All	All
Application	Tribe29	Checkmk	2.0.0	b5	All	All
Application	Tribe29	Checkmk	2.0.0	b6	All	All
Application	Tribe29	Checkmk	2.0.0	b7	All	All
Application	Tribe29	Checkmk	2.0.0	b8	All	All
Application	Tribe29	Checkmk	2.0.0	p1	All	All
Application	Tribe29	Checkmk	2.0.0	p10	All	All
Application	Tribe29	Checkmk	2.0.0	p11	All	All
Application	Tribe29	Checkmk	2.0.0	p12	All	All
Application	Tribe29	Checkmk	2.0.0	p13	All	All
Application	Tribe29	Checkmk	2.0.0	p14	All	All
Application	Tribe29	Checkmk	2.0.0	p15	All	All
Application	Tribe29	Checkmk	2.0.0	p16	All	All
Application	Tribe29	Checkmk	2.0.0	p17	All	All
Application	Tribe29	Checkmk	2.0.0	p18	All	All
Application	Tribe29	Checkmk	2.0.0	p19	All	All
Application	Tribe29	Checkmk	2.0.0	p2	All	All
Application	Tribe29	Checkmk	2.0.0	p20	All	All
Application	Tribe29	Checkmk	2.0.0	p21	All	All
Application	Tribe29	Checkmk	2.0.0	p22	All	All
Application	Tribe29	Checkmk	2.0.0	p23	All	All
Application	Tribe29	Checkmk	2.0.0	p24	All	All
Application	Tribe29	Checkmk	2.0.0	p25	All	All
Application	Tribe29	Checkmk	2.0.0	p26	All	All
Application	Tribe29	Checkmk	2.1.0	b1	All	All
Application	Tribe29	Checkmk	2.1.0	b2	All	All
Application	Tribe29	Checkmk	2.1.0	b3	All	All

Application	Tribe29	Checkmk	2.1.0	b4	All	All
Application	Tribe29	Checkmk	2.1.0	b5	All	All
Application	Tribe29	Checkmk	2.1.0	b6	All	All
Application	Tribe29	Checkmk	2.1.0	b7	All	All
Application	Tribe29	Checkmk	2.1.0	b8	All	All
Application	Tribe29	Checkmk	2.1.0	b9	All	All
Application	Tribe29	Checkmk	2.1.0	p1	All	All
Application	Tribe29	Checkmk	2.1.0	p2	All	All
Application	Tribe29	Checkmk	2.1.0	p3	All	All
Application	Tribe29	Checkmk	2.2.0	i1	All	All
cpe:2.3:a:tribe29:checkmk:1.6.0:-:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:b1:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:b10:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:b12:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:b3:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:b4:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:b5:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:b9:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p1:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p10:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p11:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p12:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p13:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p14:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p15:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p16:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p19:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p2:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p20:*:*:*:*:*:						
cpe:2.3:a:tribe29:checkmk:1.6.0:p21:*:*:*:*:*:						

cpe:2.3:a:tribe29:checkmk:1.6.0:p22:~::~~::~~::
cpe:2.3:a:tribe29:checkmk:1.6.0:p23:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0:p24:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0:p25:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0:p26:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0:p27:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0:p28:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0:p29:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0b10:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:1.6.0b11:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:-::~~::~~::~~::
cpe:2.3:a:tribe29:checkmk:2.0.0:b1:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:b2:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:b3:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:b4:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:b5:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:b6:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:b7:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:b8:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p1:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p10:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p11:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p12:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p13:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p14:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p15:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p16:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p17:~::~~::~~::~
cpe:2.3:a:tribe29:checkmk:2.0.0:p18:~::~~::~~::~

 @threatmeter	CVE-2022-33912 A permission issue affects users that deployed the shipped version of the Checkmk Debian package. Pa... twitter.com/i/web/status/1...	2022-06-18 07:09:14
 @ch2500	This has become CVE-2022-33912 - check your installs, 1.6+ are affected checkmk.com/werk/14098 twitter.com/ch2500/status/...	2022-06-19 20:21:13
 /r/netcve	CVE-2022-33912	2022-06-17 07:38:49

[← 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 registered 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