



CVE-2022-36985

Published on: Not Yet Published

Last Modified on: 08/09/2022 02:45:00 PM UTC

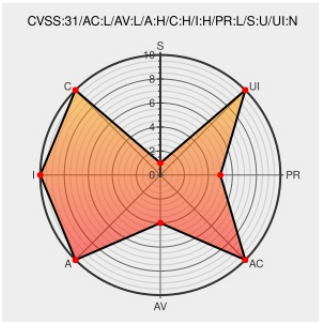
CVE-2022-36985

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Flex Appliance](#) from [Veritas](#) contain the following vulnerability:

An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x through 9.0.0.1, and 9.1.x through 9.1.0.1 (and related NetBackup products). An attacker with unprivileged local access to a Windows NetBackup Primary server could potentially escalate their privileges.

CVE-2022-36985 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



















CVE References




Description	Tags	Link
VTS22-004: HotFix for Security Advisory impacting NetBackup – Primary/Media Server Veritas™	www.veritas.com text/html	V MISC www.veritas.com/content/support/en_US/security/VTS22-004#h7

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	Veritas	Flex Appliance	1.2	All	All	All
Application	Veritas	Flex Appliance	1.3	All	All	All
Application	Veritas	Flex Appliance	2.0	All	All	All
Application	Veritas	Flex Appliance	2.0.1	All	All	All
Application	Veritas	Flex Appliance	2.0.2	All	All	All
Application	Veritas	Flex Appliance	2.1	All	All	All
Application	Veritas	Flex Scale	1.3.1	All	All	All
Application	Veritas	Flex Scale	2.1	All	All	All
Application	Veritas	Netbackup	8.1.1	All	All	All
Application	Veritas	Netbackup	8.1.2	All	All	All
Application	Veritas	Netbackup	8.2	All	All	All
Application	Veritas	Netbackup	8.3	All	All	All
Application	Veritas	Netbackup	8.3.0.1	All	All	All
Application	Veritas	Netbackup	8.3.0.2	All	All	All
Application	Veritas	Netbackup	9.0	All	All	All
Application	Veritas	Netbackup	9.0.0.1	All	All	All
Application	Veritas	Netbackup	9.1	All	All	All
Application	Veritas	Netbackup	9.1.0.1	All	All	All
Application	Veritas	Netbackup Appliance	3.1.1	All	All	All
Application	Veritas	Netbackup Appliance	3.1.2	All	All	All
Application	Veritas	Netbackup Appliance	3.2	All	All	All
Application	Veritas	Netbackup Appliance	4.0	All	All	All
Application	Veritas	Netbackup Appliance	4.1	All	All	All
Hardware  	Veritas	Netbackup Appliance	3.2	maintenance_release1	All	All
Hardware  	Veritas	Netbackup Appliance	3.2	maintenance_release2	All	All
Hardware  	Veritas	Netbackup Appliance	3.2	maintenance_release3	All	All
Hardware  	Veritas	Netbackup Appliance	3.3.0.1	maintenance_release1	All	All
Hardware  	Veritas	Netbackup Appliance	3.3.0.1	maintenance_release2	All	All
Hardware  	Veritas	Netbackup Appliance	3.3.0.2	maintenance_release1	All	All
Hardware  	Veritas	Netbackup Appliance	3.3.0.2	maintenance_release2	All	All
Hardware  	Veritas	Netbackup Appliance	4.0.0.1	maintenance_release1	All	All
Hardware  	Veritas	Netbackup Appliance	4.0.0.1	maintenance_release2	All	All

Hardware 	Veritas	Netbackup Appliance	4.0.0.1	maintenance_release3	All	All
Hardware 	Veritas	Netbackup Appliance	4.1.0.1	maintenance_release1	All	All
Hardware 	Veritas	Netbackup Appliance	4.1.0.1	maintenance_release2	All	All
cpe:2.3:a:veritas:flex_appliance:1.2:*:*:*:*:*:						
cpe:2.3:a:veritas:flex_appliance:1.3:*:*:*:*:*:						
cpe:2.3:a:veritas:flex_appliance:2.0:*:*:*:*:*:						
cpe:2.3:a:veritas:flex_appliance:2.0.1:*:*:*:*:*:						
cpe:2.3:a:veritas:flex_appliance:2.0.2:*:*:*:*:*:						
cpe:2.3:a:veritas:flex_appliance:2.1:*:*:*:*:*:						
cpe:2.3:a:veritas:flex_scale:1.3.1:*:*:*:*:*:						
cpe:2.3:a:veritas:flex_scale:2.1:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:8.1.1:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:8.1.2:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:8.2:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:8.3:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:8.3.0.1:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:8.3.0.2:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:9.0:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:9.0.0.1:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:9.1:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:9.1.0.1:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup_appliance:3.1.1:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup_appliance:3.1.2:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup_appliance:3.2:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup_appliance:4.0:*:*:*:*:*:						
cpe:2.3:a:veritas:netbackup_appliance:4.1:*:*:*:*:*:						
cpe:2.3:h:veritas:netbackup_appliance:3.2:maintenance_release1:*:*:*:*:*:						
cpe:2.3:h:veritas:netbackup_appliance:3.2:maintenance_release2:*:*:*:*:*:						
cpe:2.3:h:veritas:netbackup_appliance:3.2:maintenance_release3:*:*:*:*:*:						

cpe:2.3:h:veritas:netbackup_appliance:3.3.0.1:maintenance_release1:****:*:
cpe:2.3:h:veritas:netbackup_appliance:3.3.0.1:maintenance_release2:****:*:
cpe:2.3:h:veritas:netbackup_appliance:3.3.0.2:maintenance_release1:****:*:
cpe:2.3:h:veritas:netbackup_appliance:3.3.0.2:maintenance_release2:****:*:
cpe:2.3:h:veritas:netbackup_appliance:4.0.0.1:maintenance_release1:****:*:
cpe:2.3:h:veritas:netbackup_appliance:4.0.0.1:maintenance_release2:****:*:
cpe:2.3:h:veritas:netbackup_appliance:4.0.0.1:maintenance_release3:****:*:
cpe:2.3:h:veritas:netbackup_appliance:4.1.0.1:maintenance_release1:****:*:
cpe:2.3:h:veritas:netbackup_appliance:4.1.0.1:maintenance_release2:****:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-36985 : An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x... twitter.com/i/web/status/1...	2022-07-28 01:08:38
 @threatmeter	CVE-2022-36985 An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2, 8.3.x through 8.3.0.2, 9.x th... twitter.com/i/web/status/1...	2022-07-29 07:09:33
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-36985 - An issue was discovered in Veritas NetBackup 8.1.x through 8.1.2, 8.2... twitter.com/i/web/status/1...	2022-07-29 07:09:39

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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