

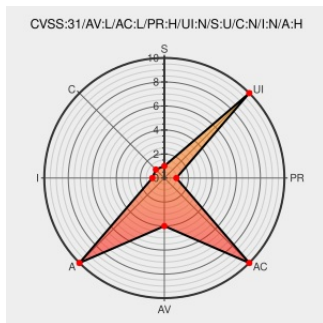


CVE-2021-38955

Published on: Not Yet Published

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-38955

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Aix](#) from [Ibm](#) contain the following vulnerability:

IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a local user with elevated privileges to cause a denial of service due to a file creation vulnerability in the audit commands. IBM X-Force ID: 211825.

CVE-2021-38955 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [IBM](#) - **VIOS** version **3.1**

Affected Vendor/Software: [IBM](#) - **AIX** version **7.1**

Affected Vendor/Software: [IBM](#) - **AIX** version **7.2**

Affected Vendor/Software: [IBM](#) - **AIX** version **7.3**

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description

Security Bulletin: Vulnerability in AIX audit commands (CVE-2021-38955)

IBM X-Force Exchange

Tags

www.ibm.com

text/html

exchange.xforce.ibmcloud.com

text/html

Link

CONFIRM

www.ibm.com/support/pages/node/6560236

XF ibm-aix-cve202138955-dos (211825)

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

330095 IBM Advanced Interactive eXecutive (AIX) File Creation Vulnerability (audit commands)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Ibm	Aix	7.1	All	All	All
Operating System	Ibm	Aix	7.2	All	All	All
Operating System	Ibm	Aix	7.3	All	All	All
Application	Ibm	Vios	3.1	All	All	All
cpe:2.3:o:ibm:aix:7.1:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:7.2:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:7.3:*:*:*:*:*:						
cpe:2.3:a:ibm:vios:3.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@softek_jp	IBM AIX の audit コマンドの処理にサービスを妨害される問題 (CVE-2021-38955) [41457] sid.softek.jp/content/show/4... #SIDfm #脆弱性情報	2022-03-01 06:35:54
@CVEreport	CVE-2021-38955 : #IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a local user with elevated privileges to cause a... twitter.com/i/web/status/1...	2022-03-01 16:51:25
/r/netcve	CVE-2021-38955	2022-03-01 17:38:43

← 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](#)