



CVE-2021-29695

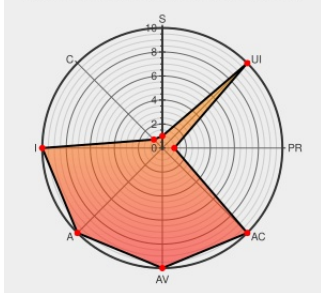
Published on: 05/25/2021 12:00:00 AM UTC

Last Modified on: 06/01/2021 01:51:00 PM UTC

CVE-2021-29695

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

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H



Certain versions of [8335-gca](#) from [ibm](#) contain the following vulnerability:

IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request that would allow them to delete arbitrary files on the system. IBM X-Force ID: 200558.

CVE-2021-29695 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [IBM](#) - **8335-GTB** version **OP820**

Affected Vendor/Software: [IBM](#) - **8335-GTA** version **OP820**

Affected Vendor/Software: [IBM](#) - **8335-GCA** version **OP820**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **8.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	COMPLETE	COMPLETE

CVE References

Security Bulletin: Mitigations are being announced to address CVE-2020-4839 and CVE-2021-29695

www.ibm.com

text/html

CONFIRM

www.ibm.com/support/pages/node/6454303

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

XF ibm-bmc-cve202129695-dir-traversal (200558)

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
Hardware 	ibm	8335-gca	-	All	All	All
Operating System	ibm	8335-gca Firmware	op820	All	All	All
Hardware 	ibm	8335-gta	-	All	All	All
Operating System	ibm	8335-gta Firmware	op820	All	All	All
Hardware 	ibm	8335-gtb	-	All	All	All
Operating System	ibm	8335-gtb Firmware	op820	All	All	All
cpe:2.3:h:ibm:8335-gca:-:*:*:*:*:*:						
cpe:2.3:o:ibm:8335-gca_firmware:op820:*:*:*:*:*:						
cpe:2.3:h:ibm:8335-gta:-:*:*:*:*:*:						
cpe:2.3:o:ibm:8335-gta_firmware:op820:*:*:*:*:*:						
cpe:2.3:h:ibm:8335-gtb:-:*:*:*:*:*:						
cpe:2.3:o:ibm:8335-gtb_firmware:op820:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-29695 : #IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on t... twitter.com/i/web/status/1...	2021-05-25 16:24:54
 /r/netcve	CVE-2021-29695	2021-05-25 16:41:38

© [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](#)