



CVE-2021-22920

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-22920
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-05 21:15:00 UTC
Updated	2021-08-13 14:26:00 UTC
Description	A vulnerability has been discovered in Citrix ADC (formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway).

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Application Delivery Management	12.1-62.25	All	All	All
Application	Citrix	Application Delivery Management	13.0-82.42	All	All	All
Application	Citrix	Gateway	12.1-62.25	All	All	All
Application	Citrix	Gateway	13.0-82.42	All	All	All

References

Reference	Source	Link
Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP Edition appliance Security Update	MISC	support.citrix.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375745](#) Citrix ADC and NetScaler Gateway Multiple Vulnerabilities(CTX319135)

[375755](#) Citrix ADC And Citrix Gateway Account Hijacking Vulnerability (CTX319135)

© [CVE.report](#) 2026 |

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](#)