



# CVE-2020-8195

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-8195
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-10 16:15:00 UTC
<b>Updated</b>	2022-09-20 17:23:00 UTC
<b>Description</b>	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 &

## Risk And Classification

**EPSS:** 0.746180000 probability, percentile 0.988440000 (date 2026-04-01)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** CWE-22

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Citrix
<b>Product</b>	Application Delivery Controller (ADC), Gateway, and SD-WAN WANOP Appliance
<b>Name</b>	Citrix ADC, Gateway, and SD-WAN WANOP Appliance Information Disclosure Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-8195">https://nvd.nist.gov/vuln/detail/CVE-2020-8195</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Citrix</a>	<a href="#">4000-wo</a>	-	All	All	All
Hardware	<a href="#">Citrix</a>	<a href="#">4000-wo</a>	-	All	All	All
Hardware	<a href="#">Citrix</a>	<a href="#">4100-wo</a>	-	All	All	All
Hardware	<a href="#">Citrix</a>	<a href="#">4100-wo</a>	-	All	All	All
Hardware	<a href="#">Citrix</a>	<a href="#">5000-wo</a>	-	All	All	All
Hardware	<a href="#">Citrix</a>	<a href="#">5000-wo</a>	-	All	All	All
Hardware	<a href="#">Citrix</a>	<a href="#">5100-wo</a>	-	All	All	All
Hardware	<a href="#">Citrix</a>	<a href="#">5100-wo</a>	-	All	All	All

Hardware	Citrix	Application Delivery Controller	-	All	All	All
Hardware	Citrix	Application Delivery Controller	-	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	All	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	All	All	All	All
Hardware	Citrix	Gateway	-	All	All	All
Hardware	Citrix	Gateway	-	All	All	All
Operating System	Citrix	Gateway Firmware	All	All	All	All
Operating System	Citrix	Gateway Firmware	All	All	All	All
Application	Citrix	Gateway Plug-in For Linux	All	All	All	All
Application	Citrix	Gateway Plug-in For Linux	All	All	All	All
Hardware	Citrix	Netscaler Gateway	-	All	All	All
Hardware	Citrix	Netscaler Gateway	-	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	All	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	All	All	All	All
Operating System	Citrix	Sd-wan Wanop	All	All	All	All
Operating System	Citrix	Sd-wan Wanop	All	All	All	All

## References

Reference	Source	Link
Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance Security Update	MISC	<a href="https://support.citrix.com">support.citrix.com</a>
Citrix ADC NetScaler Local File Inclusion ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)