



CVE-2021-1629

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

Summary

CVE	CVE-2021-1629
State	PUBLIC
Assigner	security@salesforce.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-26 17:15:00 UTC
Updated	2021-06-03 18:58:00 UTC
Description	Tableau Server fails to validate certain URLs that are embedded in emails sent to Tableau Server users.

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Tableau	Tableau Server	All	All	All	All

References

Reference	Source	Link	Tags
Help Training Salesforce	MISC	help.salesforce.com	
Full Disclosure: [SYSS-2020-032] Open Redirect in Tableau Server (CVE-2021-1629)	FULLDISC	seclists.org	
Tableau Server Open Redirection ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375433](#) Tableau Server Multiple Vulnerabilities (ADV-2021-010,ADV-2021-011,ADV-2021-012)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)