



CVE-2020-28351

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

Summary

CVE	CVE-2020-28351
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-09 04:15:00 UTC
Updated	2020-11-18 15:15:00 UTC
Description	The conferencing component on Mitel ShoreTel 19.46.1802.0 devices could allow an unauthenticated attacker to conduct a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Mitel	Shoretel	-	All	All	All
Hardware	Mitel	Shoretel	-	All	All	All
Operating System	Mitel	Shoretel Firmware	19.46.1802.0	All	All	All
Operating System	Mitel	Shoretel Firmware	19.46.1802.0	All	All	All

References

Reference	Source
ShoreTel Conferencing 19.46.1802.0 Cross Site Scripting ≈ Packet Storm	MISC
GitHub - dievus/CVE-2020-28351: CVE-2020-28351 - Reflected Cross-Site Scripting attack in ShoreTel version 19.46.1802.0.	MISC
Attention Required! Cloudflare	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#) 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](#)