



CVE-2019-19266

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

Summary

CVE	CVE-2019-19266
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-06 00:15:00 UTC
Updated	2020-01-08 14:50:00 UTC
Description	IceWarp WebMail Server 12.2.0 and 12.1.x before 12.2.1.1 (and probably earlier versions) allows XSS (issue 2 of 2) in note

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Icewarp	Mail Server	All	All	All	All
Application	Icewarp	Mail Server	All	All	All	All

References

Reference	Source	Link	Tags
Full Disclosure: [RT-SA-2019-016] IceWarp: Cross-Site Scripting in Notes	MISC	seclists.org	Exploit, Mailing List, T
RedTeam Pentesting GmbH - IceWarp: Cross-Site Scripting in Notes	CONFIRM	www.redteam-pentesting.de	Exploit, Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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