CVE-2020-29444

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-29444
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-07 06:15:00 UTC
Updated	2022-07-27 14:05:00 UTC
Description	Affected versions of Team Calendar in Confluence Server before 7.11.0 allow attackers to inject arbitrary HTML or Javascri

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Confluence	All	All	All	All
Application	Atlassian	Confluence Data Center	All	All	All	All
Application	Atlassian	Confluence Server	All	All	All	All
Application	Atlassian	Data Center	All	All	All	All

References

Reference
[CONFSERVER-61266] Persistent XSS through Team Calendar in Confluence Server - CVE-2020-29444 - Create and track feature requests
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730477 Atlassian Confluence Cross-Site Scripting (XSS) Vulnerability (CONFSERVER-61266)