



CVE-2019-20104

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

Summary

CVE	CVE-2019-20104
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-06 03:15:00 UTC
Updated	2022-01-01 19:56:00 UTC
Description	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote at

Risk And Classification

Problem Types: CWE-776

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Crowd	All	All	All	All
Application	Atlassian	Crowd	All	All	All	All

References

Reference	Source	L
CVE-2019-20104 – Atlassian Crowd OpenID client vulnerable to Remote DoS via XML Entity Expansion – ZeroAuth	MISC	z
[CWD-5526] XXE in OpenID client application - CVE-2019-20104 - Create and track feature requests for Atlassian products.	N/A	jr
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

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](#).

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