CVE-2019-3398

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-3398
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-18 18:29:00 UTC
Updated	2022-04-12 18:39:00 UTC
Description	Confluence Server and Data Center had a path traversal vulnerability in the downloadallattachments resource. A remote att

Risk And Classification

EPSS: 0.938540000 probability, percentile 0.998700000 (date 2026-05-08)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Atlassian
Product	Confluence Server and Data Center
Name	Atlassian Confluence Server and Data Center Path Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-3398

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Confluence Server / Data Center Path Traversal ≈ Packet Storm
[CONFSERVER-58102] Confluence - Path traversal vulnerability - CVE-2019-3398 - Create and track feature requests for Atlassian products.

Atlassian Confluence Server and Confluence Data Center Directory Traversal Vulnerability
Atlassian Confluence 6.15.1 Directory Traversal ≈ Packet Storm
Atlassian Confluence 6.15.1 Directory Traversal ≈ Packet Storm
Bugtraq: Confluence Security Advisory - 2019-04-17
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**