CVE-2021-43957

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-43957
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-16 01:15:00 UTC
Updated	2022-03-22 16:01:00 UTC
Description	Affected versions of Atlassian Fisheye & Crucible allowed remote attackers to browse local files via an Insecure Direct Obje

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Fisheye	All	All	All	All

References

Reference
[FE-7388] CVE-2021-43957: Bypass for CVE-2020-29446 (Local file disclosure / path traversal within WEB-INF) - Create and track feature rec
[CRUC-8524] CVE-2021-43957: Bypass for CVE-2020-29446 (Local file disclosure / path traversal within WEB-INF) - Create and track feature
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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