CVE-2019-14852

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-14852
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-18 20:15:00 UTC
Updated	2021-06-04 12:07:00 UTC
Description	A flaw was found in 3scale's APIcast gateway that enabled the TLS 1.0 protocol. An attacker could target traffic using this w

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	3scale Api Management	2.0	All	All	All
Application	Redhat	3scale Api Management Platform	2.0	All	All	All

References

Reference	Source	Link
1758208 – (CVE-2019-14852) CVE-2019-14852 apicast: deprecated protocol TLS 1.0 enabled in gateway	MISC	bugzilla.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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