CVE-2017-18362

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

Summary

CVE	CVE-2017-18362
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-05 06:29:00 UTC
Updated	2019-02-22 18:33:00 UTC
Description	ConnectWise ManagedITSync integration through 2017 for Kaseya VSA is vulnerable to unauthenticated remote command

Risk And Classification

EPSS: 0.802990000 probability, percentile 0.991290000 (date 2026-05-02)

CISA KEV: Listed on 2022-05-24; due 2022-06-14; ransomware use Known

Problem Types: CWE-89

CISA Known Exploited Vulnerability

Vendor	Kaseya
Product	Virtual System/Server Administrator (VSA)
Name	Kaseya VSA SQL Injection Vulnerability
Required Action	The impacted product is end-of-life and should be disconnected if still in use.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-18362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Connectwise	Manageditsync	All	All	All	All

References

Reference	Source	Link
archive.today/rdkeQ	MISC	archive.today
Error 404 (Not Found)!!1	MISC	webcache.googleusercc
GitHub - kbni/owlky: Proof of concept exploit for ManagedITSync (Kaseya & ConnectWise integration)	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org

NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

731317 Kaseya VSA Remote Code Execution (RCE) Vulnerability