



CVE-2021-30116

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

Summary

CVE	CVE-2021-30116
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-09 14:15:00 UTC
Updated	2023-10-23 14:15:00 UTC
Description	Kaseya VSA before 9.5.7 allows credential disclosure, as exploited in the wild in July 2021. By default Kaseya VSA on pren

Risk And Classification

EPSS: 0.540740000 probability, percentile 0.980400000 (date 2026-05-17)

CISA KEV: Listed on 2021-11-03; due 2021-11-17; ransomware use Known

Problem Types: CWE-522

CISA Known Exploited Vulnerability

Vendor	Kaseya
Product	Virtual System/Server Administrator (VSA)
Name	Kaseya Virtual System/Server Administrator (VSA) Information Disclosure Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-30116

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaseya	Vsa	All	All	All	All
Application	Kaseya	Vsa Agent	All	All	All	All
Application	Kaseya	Vsa Server	All	All	All	All

References

Reference	Source	Link	Tags
Important Notice July 7th, 2021 – Kaseya	MISC	helpdesk.kaseya.com	
Kaseya VSA REvil Ransomware Attack 2021 - ransomware attacks 2021	MISC	www.secpod.com	

Kaseya VSA Limited Disclosure DIVD CSIRT	MISC	csirt.divd.nl	
Kaseya Case Update 2 DIVD CSIRT	MISC	csirt.divd.nl	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

Vendor Comments And Credit

Discovery Credit

LEGACY: Discovered by Wietse Boonstra of DIVD

LEGACY: Additional research by Frank Breedijk of DIVD

Legacy QID Mappings

[730134](#) Kaseya VSA Remote Code Execution Vulnerability (Zero Day)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API cve.report/api

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