



CVE-2015-6922

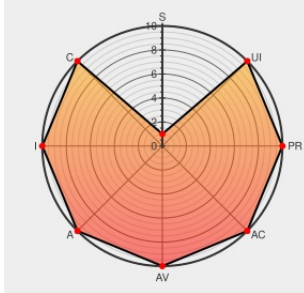
Published on: 02/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6922

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Virtual System Administrator](#) from [Kaseya](#) contain the following vulnerability:

Kaseya Virtual System Administrator (VSA) 7.x before 7.0.0.33, 8.x before 8.0.0.23, 9.0 before 9.0.0.19, and 9.1 before 9.1.0.9 does not properly require authentication, which allows remote attackers to bypass authentication and (1) add an administrative account via crafted request to LocalAuth/setAccount.aspx or (2) write to and execute arbitrary files via a full pathname in the PathData parameter to ConfigTab/uploader.aspx.

CVE-2015-6922 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Kaseya Virtual System Administrator Code Execution / Privilege Escalation ~ Packet Storm	Exploit Third Party Advisory	MISC packetstormsecurity.com/files/133782/Kaseya-Virtual-System-Administrator-Code-Execution-Privilege-Escalation/

	VDB Entry packetstormsecurity.com text/html	Escalation.html
Kaseya Virtual System Administrator (VSA) - Multiple Vulnerabilities (2) - ASP webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	 MISC www.exploit-db.com/exploits/38351/
Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-15-448
Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-15-449
Kaseya Security Advisory : Kaseya	Broken Link Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 MISC helpdesk.kaseya.com/entries/96164487--Kaseya-Security-Advisory
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report .		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaseya	Virtual System Administrator	All	All	All	All
Application	Kaseya	Virtual System Administrator	All	All	All	All
cpe:2.3:a:kaseya:virtual_system_administrator:*:*:*:*:*:						
cpe:2.3:a:kaseya:virtual_system_administrator:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

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