CVE-2021-30119 - AUTHENTICATED AUTHENTICATED REFLECTIVE XSS IN KASEYA VSA <= V9.5.6

CVE	[CVE-2021-30119](CVE-2021-30119)
Case	DIVD-2021-00011
Discovered by	• Wietse Boonstra
Credits	• Discovered by Wietse Boonstra of DIVD • Additional research by Frank Breedijk and Hidde Smit of DIVD
Products	Kaseya: • Kaseya VSA
Versions	Kaseya: • Kaseya VSA • 9.x (<= 9.5.6)
CVSS	Base score: [5.4](5.4)
References	• https://csirt.divd.nl/2021/07/07/Kaseya-Limited-Disclosure/ • https://csirt.divd.nl/DIVD-2021-00011

- https://csirt.divd.nl/CVE-2021-30119

Solution	Upgrade to a version above 9.5.6
Last modified	14 Dec 2022 20:32

DESCRIPTION

Authenticated reflective XSS in HelpDeskTab/rcResults.asp

The parameter result of /HelpDeskTab/rcResults.asp is insecurely returned in the requested web page and can be used to perform a Cross Site Scripting attack

Example request: `https://x.x.x.x/HelpDeskTab/rcResults.asp?result=<script>alert(document.cookie)</script>`

The same is true for the parameter FileName of /done.asp

Eaxmple request: `https://x.x.x.x/done.asp?FileName=";</script><script>alert(1);a="&PathData=&originalName=shell.aspx&FileSize=4388&TimeElapsed=00:00:00.078`

Image 1. Screenshot of XSS

[JSON version](#)