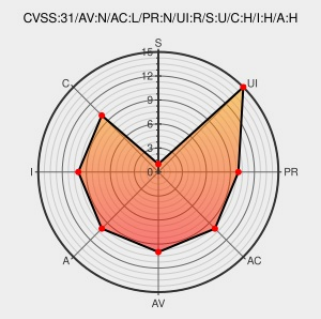
CVE-2017-15049

Published on: 12/19/2017 12:00:00 AM UTC

Last Modified on: 05/14/2021 03:14:00 PM UTC

CVE-2017-15049

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Zoom from Zoom contain the following vulnerability:

The ZoomLauncher binary in the Zoom client for Linux before 2.0.115900.1201 does not properly sanitize user input when constructing a shell command, which allows remote attackers to execute arbitrary code by leveraging the zoommtg:// scheme handler.

CVE-2017-15049 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
advisories/CONVISO-17-003.txt at master · convisoappsec/advisories · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/convisoappsec/advisories/blob/master/2017/CONVISO-17-003.txt

Full Disclosure: [CONVISO-17-003] - Zoom Linux Client Command Injection Vulnerability (RCE)	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20171215 [CONVISO-17-003] - Zoom Linux Client Command Injection Vulnerability (RCE)
Zoom Linux Client 2.0.106600.0904 - Command Injection - Linux dos Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43354
Zoom Linux Client 2.0.106600.0904 Command Injection ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/145453/Zoom-Linux-Client-2.0.106600.0904-Command-Injection.html

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	Zoom	Zoom	All	All	All	All
Application	Zoom	Zoom Client	All	All	All	All
Application	Zoom	Zoom Client	All	All	All	All

cpe:2.3:a:zoom:zoom:*:*:*:*:*:linux:*:*:

cpe:2.3:a:zoom:zoom_client:*:*:*:*:*:linux:*:*:

cpe:2.3:a:zoom:zoom_client:*:*:*:*:*:linux:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→