



CVE-2017-18635

Published on: 09/25/2019 12:00:00 AM UTC

Last Modified on: 04/06/2022 05:54:00 PM UTC

CVE-2017-18635

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

An XSS vulnerability was discovered in noVNC before 0.6.2 in which the remote VNC server could inject arbitrary HTML into the noVNC web page via the messages propagated to the status field, such as the VNC server name.

CVE-2017-18635 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 2854-1] novnc security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20211228 [SECURITY] [DLA 2854-1] novnc security update
GitHub - ShielderSec/cve-2017-18635: PoC for CVE-	github.com text/html	MISC github.com/ShielderSec/cve-2017-18635

2017-18635

Bug #1656435 "XSS in noVNC" : Bugs : OpenStack Dashboard (Horizon)

[Issue Tracking](#)
[Third Party Advisory](#)
[bugs.launchpad.net](#)
[text/html](#)

 [MISC bugs.launchpad.net/horizon/+bug/1656435](https://bugs.launchpad.net/horizon/+bug/1656435)

[SECURITY] [DLA 1946-1] novnc security update

[lists.debian.org](#)
[text/html](#)

 [MLIST \[debian-lts-announce\] 20191005 \[SECURITY\] \[DLA 1946-1\] novnc security update](#)

[Fixed] XSS Vulnerability in noVNC · Issue #748 · novnc/noVNC · GitHub

[Patch](#)
[Third Party Advisory](#)
[github.com](#)
[text/html](#)

 [MISC github.com/novnc/noVNC/issues/748](https://github.com/novnc/noVNC/issues/748)

Red Hat Customer Portal

[access.redhat.com](#)
[text/html](#)

 [REDHAT RHSA-2020:0754](#)

Use textContent instead of innerHTML · novnc/noVNC@6048299 · GitHub

[Patch](#)
[Third Party Advisory](#)
[github.com](#)
[text/html](#)

 [MISC github.com/novnc/noVNC/commit/6048299a138e078aed210f163111698c8c526a13#diff-286f7dc7b881e942e97cd50c10898f03L534](#)

USN-4522-1: noVNC vulnerability | Ubuntu security notices | Ubuntu

[usn.ubuntu.com](#)
[text/html](#)

 [UBUNTU USN-4522-1](#)

Exploiting an old noVNC XSS (CVE-2017-18635) in OpenStack - Shielder

[www.shielder.it](#)
[text/html](#)

 [MISC www.shielder.it/blog/exploiting-an-old-novnc-xss-cve-2017-18635-in-openstack/](#)

Release v0.6.2 · novnc/noVNC · GitHub

[Release Notes](#)
[Third Party Advisory](#)
[github.com](#)
[text/html](#)

 [MISC github.com/novnc/noVNC/releases/tag/v0.6.2](https://github.com/novnc/noVNC/releases/tag/v0.6.2)

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.

Related QID Numbers

[178968](#) Debian Security Update for novnc (DLA 2854-1)

[198198](#) Ubuntu Security Notification for noVNC vulnerability (USN-4522-1)

[980721](#) Nodejs (npm) Security Update for @novnc/novnc (GHSA-49rv-g7w5-m8xx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Novnc	Novnc	All	All	All	All

Application	Novnc	Novnc	All	All	All	All
Application	Redhat	Openstack	13	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:16.04:.*.*:esm:.*.*:						
cpe:2.3:o:debian:debian_linux:8.0:.*.*.*.*.*:						
cpe:2.3:o:debian:debian_linux:9.0:.*.*.*.*.*:						
cpe:2.3:a:novnc:novnc:.*.*.*.*.*:						
cpe:2.3:a:novnc:novnc:.*.*.*.*.*:						
cpe:2.3:a:redhat:openstack:13:.*.*.*.*.*:						

No vendor comments have been submitted for this CVE