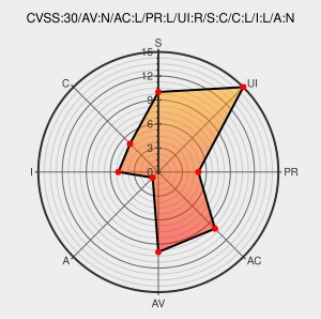
CVE-2020-29497

Published on: 01/04/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-29497

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



Certain versions of Wyse Management Suite from Dell contain the following vulnerability:

Dell Wyse Management Suite versions prior to 3.1 contain a stored cross-site scripting vulnerability. A remote authenticated malicious user with low privileges could exploit this vulnerability to store malicious HTML or JavaScript code under the device tag. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.

CVE-2020-29497 has been assigned by secure@dell.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Dell** - **Wyse Management Suite** version **< 3.1**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link

DSA-2020-282: Dell Wyse Management Suite Security Update for Multiple Vulnerabilities | Dell US

Vendor Advisory
web.archive.org
text/html
Inactive Link Not Archived

MISC
www.dell.com/support/kbdoc/en-us/000180983/dsa-2020-282

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dell	Wyse Management Suite	All	All	All	All
Application	Dell	Wyse Management Suite	All	All	All	All

cpe:2.3:a:dell:wyse_management_suite:*:*:*:*:*:*:*:*:

cpe:2.3:a:dell:wyse_management_suite:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→