



CVE-2017-17425

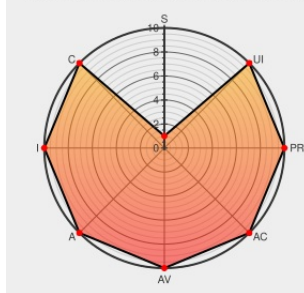
Published on: 02/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-17425

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Netvault Backup](#) from [Quest](#) contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Quest NetVault Backup 11.3.0.12.

Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of NVBUSourceDeviceSet Get method requests. The issue results from the lack of proper validation of a user-

supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of the underlying database. Was ZDI-CAN-4237.

CVE-2017-17425 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Quest - Quest NetVault Backup** version 11.3.0.12

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

ZDI-17-987 | Zero Day Initiative

Tags

Third Party Advisory

VDB Entry

zerodayinitiative.com

text/html

Link

 MISC zerodayinitiative.com/advisories/ZDI-17-987

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	Quest	Netvault Backup	11.3.0.12	All	All	All
Application	Quest	Netvault Backup	11.3.0.12	All	All	All

cpe:2.3:a:quest:netvault_backup:11.3.0.12:*****:

cpe:2.3:a:quest:netvault_backup:11.3.0.12:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →