



CVE-2018-11171

Published on: 06/01/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11171

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

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

Quest DR Series Disk Backup software version before 4.0.3.1 allows command injection (issue 29 of 46).

CVE-2018-11171 has been assigned by [M](#) 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	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Quest DR Series Disk Backup Multiple Vulnerabilities SecureAuth	Technical Description Third Party Advisory www.coresecurity.com text/html	MISC www.coresecurity.com/advisories/quest-dr-series-disk-backup-multiple-vulnerabilities

 [MISC packetstormsecurity.com/files/148003/Quest-DR-Series-Disk-Backup-Software-4.0.3-Code-Execution.html](https://packetstormsecurity.com/files/148003/Quest-DR-Series-Disk-Backup-Software-4.0.3-Code-Execution.html)

FULLDISC 20180531 [CORE-2018-0002] - Quest DR
Series Disk Backup Multiple Vulnerabilities

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quest	Disk Backup	All	All	All	All
Application	Quest	Disk Backup	All	All	All	All
<pre>cpe:2.3:a:quest:disk_backup:*****:.*:</pre>						
<pre>cpe:2.3:a:quest:disk_backup:*****:.*:</pre>						

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE.report and Source URL Uptime Status status.cve.report