



CVE-2021-42550

Published on: Not Yet Published

Last Modified on: 12/12/2022 09:13:00 PM UTC

CVE-2021-42550

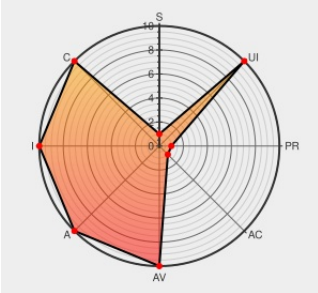
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H



Certain versions of **Cloud Manager** from **Netapp** contain the following vulnerability:

In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.

CVE-2021-42550 has been assigned by vulnerability@ncsc.ch to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **QOS.ch** - **logback** version < 1.2.9

Affected Vendor/Software: **QOS.ch** - **logback** version < 1.3.0-alpha11

CVSS3 Score: **6.6 - MEDIUM**

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

CVSS2 Score: **8.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-371761.pdf
[LOGBACK-1591] Possibility of vulnerability - QOS.ch JIRA	jira.qos.ch text/html	MISC jira.qos.ch/browse/LOGBACK-1591
Full Disclosure: Open-Xchange Security Advisory 2022-07-21	seclists.org text/html	FULLDISC 20220721 Open-Xchange Security Advisory 2022-07-21
CVE-2021-42550 Logback Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20211229-0001/
GitHub - cn-panda/logbackRceDemo: The project is a simple vulnerability Demo environment written by SpringBoot. Here, I deliberately wrote a vulnerability environment where there are arbitrary file uploads, and then use the `scan` attribute in the loghack configuration file to cooperate with the logback vulnerability to implement RCE.	github.com text/html	MISC github.com/cn-panda/logbackRceDemo
Open-Xchange App Suite 7.10.x Cross Site Scripting / Command Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/167794/Open-Xchange-App-Suite-7.10.x-Cross-Site-Scripting-Command-Injection.html
Logback News	logback.qos.ch text/html	CONFIRM logback.qos.ch/news.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.

Related QID Numbers

- [240566 Red Hat Update for Satellite 6.11 Release \(RHSA-2022:5498\)](#)
- [591301 Siemens SINEC NMS Arbitrary Code Execution Vulnerability \(SSA-371761 V1.0.3\)](#)
- [960505 Rocky Linux Security Update for Satellite \(RLSA-2022:5498\)](#)

Exploit/POC from Github

Fastest filesystem scanner for log4shell (CVE-2021-44228, CVE-2021-45046) and other vulnerable (CVE-2017-5645, CVE-20...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Cloud Manager	-	All	All	All
Application	Netapp	Service Level Manager	-	All	All	All
Application	Netapp	Snap Creator Framework	-	All	All	All
Application	Qos	Logback	1.3.0	alpha0	All	All
Application	Qos	Logback	1.3.0	alpha1	All	All
Application	Qos	Logback	1.3.0	alpha10	All	All

Social mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-42550 : In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit conf... twitter.com/i/web/status/1...	2021-12-16 18:25:35
 /r/netcve	CVE-2021-42550	2021-12-16 19:38:33

[← Previous ID](#)[Next ID→](#)

© CVE.report 2023   |

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, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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