



CVE-2022-21290

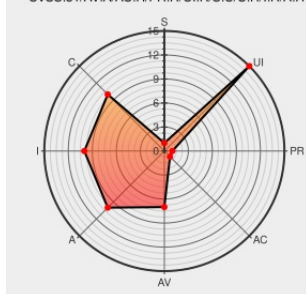
Published on: 01/19/2022 12:00:00 AM UTC

Last Modified on: 01/22/2022 03:21:00 AM UTC

CVE-2022-21290

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

CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Oncommand Insight](#) from [Netapp](#) contain the following vulnerability:

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVE-2022-21290 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Oracle Corporation - MySQL Cluster** version = **8.0.27 and prior**

CVSS3 Score: **6.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	HIGH	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	HIGH	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ZDI-22-086 Zero Day Initiative	www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-22-086/
Oracle Critical Patch Update Advisory - January 2022	www.oracle.com text/html	 MISC www.oracle.com/security-alerts/cpujan2022.html
January 2022 MySQL Server Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20220121-0008/

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

[900532](#) Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (7504)

[901766](#) Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (7546-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Oracle	Mysql	All	All	All	All
cpe:2.3:a:netapp:oncommand_insight:-:*:*:*:*:*:						
cpe:2.3:a:netapp:oncommand_workflow_automation:-:*:*:*:*:*:						
cpe:2.3:a:oracle:mysql:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @prophaze	Oracle MySQL Cluster up to 8.0.27 Privilege Escalation [CVE-2022-21290] prophaze.com/cve/oracle-mys... #Exploit:No #Local:... twitter.com/i/web/status/1...	2022-01-19 15:05:55

[← Previous ID](#)

[Next ID →](#)

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](#)