



CVE-2022-23235

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-23235
State	PUBLIC
Assigner	security-alert@netapp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-25 18:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.10P1 are susceptible to a

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	9.10	-	All	All
Application	Netapp	Active Iq Unified Manager	9.10	-	All	All
Application	Netapp	Active Iq Unified Manager	9.10	-	All	All

References

Reference	Source	Link
CVE-2022-23235 Information Disclosure Vulnerability in Active IQ Unified Manager NetApp Product Security	MISC	security.netapp.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377594](#) Active IQ Unified Manager Unauthenticated Information Disclosure Vulnerability (NTAP-20220324-0001)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)