



CVE-2022-3116

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-3116
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-27 22:15:00 UTC
Updated	2023-05-05 20:15:00 UTC
Description	The Heimdal Software Kerberos 5 implementation is vulnerable to a null pointer dereference. An attacker with network access

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Heimdal Project	Heimdal	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2022-3116 Heimdal Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
VU#730793 - Heimdal Kerberos vulnerable to remotely triggered NULL pointer dereference	MISC	www.kb.cert.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[198986](#) Ubuntu Security Notification for Heimdal Vulnerabilities (USN-5675-1)

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](#)