Squid has issues in ICP message handling

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33515
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 01:16:27 UTC
Updated	2026-03-31 01:22:04 UTC
Description	Squid is a caching proxy for the Web. Prior to version 7.5, due to improper input validation, Squid is vulnerable to out of bou

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001530000 probability, percentile 0.359240000 (date 2026-04-01)

Problem Types: CWE-125 | CWE-1289 | CWE-125 CWE-125: Out-of-bounds Read | CWE-1289 CWE-1289: Improper Validation of Unsafe Equivalence in Input

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/S
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/S
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squid-cache	Squid	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Squid-cache	Squid	affected < 7.5	Not specified

References

Reference	Source	Link
github.com/squid-cache/squid/pull/2220	security-advisories@github.com	github.co
github.com/squid-cache/squid/security/advisories/GHSA-84p4-hcx7-jj7c	security-advisories@github.com	github.co
www.openwall.com/lists/oss-security/2026/03/25/4	af854a3a-2127-422b-91ae-364da2661108	www.ope
github.com/squid-cache/squid/pull/2220	security-advisories@github.com	github.co
github.com/squid-cache/squid/commit/8138e909d2058d4401e0ad49b583afaec912...	security-advisories@github.com	github.co
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.