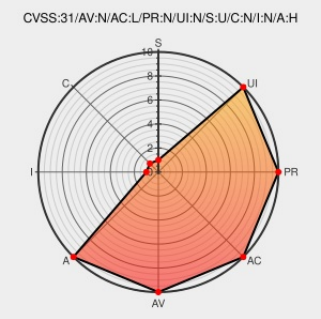
CVE-2020-14148

Published on: 06/15/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 06:59:00 PM UTC

CVE-2020-14148

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ngircd from Barton contain the following vulnerability:

The Server-Server protocol implementation in ngIRCd before 26~rc2 allows an out-of-bounds access, as demonstrated by the IRC_NJOIN() function.

CVE-2020-14148 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Release ngIRCd 26~rc2 · ngircd/ngircd · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/ngircd/ngircd/releases/tag/rel-26-rc2

Client_Search: Avoid crash if Nick == NULL. by hillu · Pull Request #275 · ngircd/ngircd · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ngircd/ngircd/pull/275
[SECURITY] [DLA 2252-1] ngircd security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200621 [SECURITY] [DLA 2252-1] ngircd security update
[SECURITY] Fedora 32 Update: ngircd-26-3.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-e6d1d849c5
[SECURITY] Fedora 31 Update: ngircd-26-3.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-8c33e3a771
Conn_Write: out-of-bounds index access (AFL + libdislocate) · Issue #277 · ngircd/ngircd · GitHub	Third Party Advisory github.com text/html	MISC github.com/ngircd/ngircd/issues/277
Avoid calling IRC_KillClient with Client == NULL by hillu · Pull Request #276 · ngircd/ngircd · GitHub	Third Party Advisory github.com text/html	MISC github.com/ngircd/ngircd/pull/276
iconv-related crash (AFL) · Issue #274 · ngircd/ngircd · GitHub	Third Party Advisory github.com text/html	MISC github.com/ngircd/ngircd/issues/274

Related QID Numbers

500430 Alpine Linux Security Update for ngircd

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Barton	Ngircd	26.0	rc1	All	All
Application	Barton	Ngircd	26.0	rc1	All	All
Application	Barton	Ngircd	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All

cpe:2.3:a:barton:ngircd:26.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:26.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:*:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→