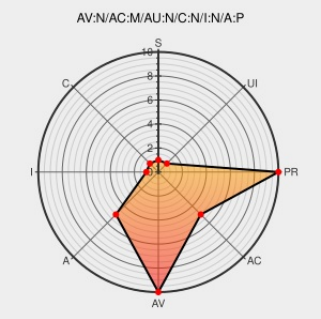
CVE-2013-5580

Published on: 10/01/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

CVE-2013-5580

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



Certain versions of Ngircd from Barton contain the following vulnerability:

The (1) Conn_StartLogin and (2) cb_Read_Resolver_Result functions in conn.c in ngIRCd 18 through 20.2, when the configuration option NoticeAuth is enabled, does not properly handle the return code for the Handle_Write function, which allows remote attackers to cause a denial of service (assertion failure and server crash) via unspecified vectors, related to a "notice auth" message not being sent to a new client.

CVE-2013-5580 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 18 Update: ngircd-20.3-1.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-15290
[ngIRCd-ML] ngIRCd 20.3	arthur.barton.de text/html	MLIST [ngircd-ml] 20130823 ngIRCd 20.3
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 96590
Security Advisory SA54567 - ngIRCd "Handle_Write" Denial of Service Vulnerabilities - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 54567

All releases of ngIRCd – Freecode	Patch freecode.com text/html	CONFIRM freecode.com/projects/ngircd/releases/357245
arthur.barton.de Git - ngircd.git/commit	Patch arthur.barton.de text/xml	CONFIRM arthur.barton.de/cgi-bin/gitweb.cgi?p=ngircd.git;a=commit;h=309122017ebc6fff039a7cab1b82f632853d82d5
[SECURITY] Fedora 19 Update: ngircd-20.3-1.fc19	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-15278

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Barton	Ngircd	18.0	All	All	All
Application	Barton	Ngircd	19.0	All	All	All
Application	Barton	Ngircd	19.1	All	All	All
Application	Barton	Ngircd	20.0	All	All	All
Application	Barton	Ngircd	20.1	All	All	All
Application	Barton	Ngircd	20.2	All	All	All
Application	Barton	Ngircd	18.0	All	All	All
Application	Barton	Ngircd	19.0	All	All	All
Application	Barton	Ngircd	19.1	All	All	All
Application	Barton	Ngircd	20.0	All	All	All
Application	Barton	Ngircd	20.1	All	All	All
Application	Barton	Ngircd	20.2	All	All	All

cpe:2.3:a:barton:ngircd:18.0:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:19.0:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:19.1:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:20.0:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:20.1:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:20.2:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:18.0:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:19.0:*:*:*:*:*:*:*:

cpe:2.3:a:barton:ngircd:19.1:*:*:*:*:*:*:*

cpe:2.3:a:barton:ngircd:20.0:*:*:*:*:*:*:*

cpe:2.3:a:barton:ngircd:20.1:*:*:*:*:*:*:*

cpe:2.3:a:barton:ngircd:20.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→