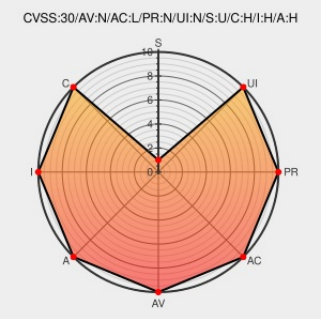
CVE-2017-8289

Published on: 04/26/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:43 PM UTC

CVE-2017-8289

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



Certain versions of Riot from Riot Project contain the following vulnerability:

Stack-based buffer overflow in the ipv6_addr_from_str function in sys/net/network_layer/ipv6/addr/ipv6_addr_from_str.c in RIOT prior to 2017-04-25 allows local attackers, and potentially remote attackers, to cause a denial of service or possibly have unspecified other impact via a malformed IPv6 address.

CVE-2017-8289 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Stack Buffer Overflow - Potential Denial of Service · Issue #6840 · RIOT-OS/RIOT · GitHub	Issue Tracking, Patch, Third Party Advisory	CONFIRM github.com/RIOT-OS/RIOT/issues/6840

	github.com text/html	
ipv6_addr: provide fix for off-by-x error [2017.04 backport] by miri64 · Pull Request #6962 · RIOT-OS/RIOT · GitHub	Issue Tracking Patch github.com text/html	CONFIRM github.com/RIOT-OS/RIOT/pull/6962
ipv6_addr: provide fix for off-by-x error by miri64 · Pull Request #6961 · RIOT-OS/RIOT · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/RIOT-OS/RIOT/pull/6961

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:riot_project:riot:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→