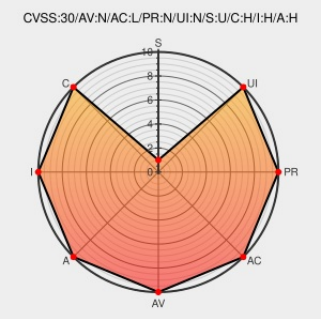
CVE-2017-9430

Published on: 06/05/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:57 PM UTC

CVE-2017-9430

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



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

Stack-based buffer overflow in dnstracer through 1.9 allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a command line with a long name argument that is mishandled in a strcpy call for argv[0]. An example threat model is a web application that launches dnstracer with an untrusted name string.

CVE-2017-9430 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
DNSTracer Stack-based Buffer Overflow - CXSecurity.com	Third Party Advisory cxsecurity.com	MISC cxsecurity.com/issue/WLB-2017060030

	text/html	
DNSTracer 1.9 - Local Buffer Overflow - Linux local Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 42424
DNSTracer 1.8.1 - Buffer Overflow	Third Party Advisory www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 42115
DNSTracer 1.8.1 Buffer Overflow ≈ Packet Storm	Third Party Advisory packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/142799/DNSTracer-1.8.1-Buffer-Overflow.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:dnstracer_project:dnstracer:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→