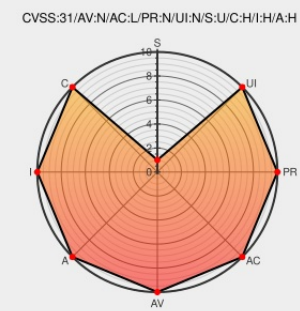
CVE-2021-44847

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2021-44847

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



Certain versions of Toxcore from Digitalocean contain the following vulnerability:

A stack-based buffer overflow in handle_request function in DHT.c in toxcore 0.1.9 through 0.1.11 and 0.2.0 through 0.2.12 (caused by an improper length calculation during the handling of received network packets) allows remote attackers to crash the process or potentially execute arbitrary code via a network packet.

CVE-2021-44847 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
[SECURITY] Fedora 34 Update: toxcore-0.2.13-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-8b746a32c5
[SECURITY] Fedora 35 Update: toxcore-0.2.13-1.fc35 - package-announce -	lists.fedoraproject.org	FEDORA FEDORA-2021-

[SECURITY] Fedora 33 Update: toxcore-0.2.13-1.fc33 - package-announce Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-8026e9b394
fix: Sec/fix crypto size compute by sudden6 · Pull Request #1718 · TokTok/c-toxcore · GitHub	github.com text/html	MISC github.com/TokTok/c-toxcore/pull/1718

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

183946 Debian Security Update for libtoxcore (CVE-2021-44847)

282197 Fedora Security Update for toxcore (FEDORA-2021-8b746a32c5)

282199 Fedora Security Update for toxcore (FEDORA-2021-8026e9b394)

751569 OpenSUSE Security Update for c-toxcore (openSUSE-SU-2021:1640-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digitalocean	Toxcore	All	All	All	All
Application	Digitalocean	Toxcore	All	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Toktok	Toxcore	All	All	All	All
Application	Toktok	Toxcore	All	All	All	All

cpe:2.3:a:digitalocean:toxcore:*:*:*:*:*:*:*:*:

cpe:2.3:a:digitalocean:toxcore:*:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:a:toktok:toxcore:*:*:*:*:*:*:*:*:

cpe:2.3:a:toktok:toxcore:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2021-44847	2021-12-13 02:38:18

/r/projecttox	Stack-based buffer overflow vulnerability in UDP packet handling in Toxcore (CVE-2021-44847)	2021-12-13 22:21:43

← Previous ID

Next ID→