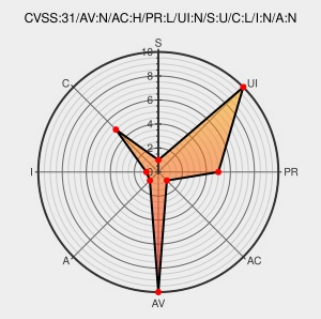
CVE-2018-25022

Published on: 12/12/2021 12:00:00 AM UTC

Last Modified on: 02/08/2022 06:55:00 PM UTC

CVE-2018-25022

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



Certain versions of Toxcore from Digitalocean contain the following vulnerability:

The Onion module in toxcore before 0.2.2 doesn't restrict which packets can be onion-routed, which allows a remote attacker to discover a target user's IP address (when knowing only their Tox Id) by positioning themselves close to target's Tox Id in the DHT for the target to establish an onion connection with the attacker, guessing the target's DHT public key and creating a DHT node with public key close to it, and finally onion-routing a NAT Ping Request to the target, requesting it to ping the just created DHT node.

CVE-2018-25022 has been assigned by cve@mitre.org to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.1 - LOW

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Onion vulnerability · Issue #873 · TokTok/c-toxcore · GitHub		MISC github.com/TokTok/c

Onion vulnerability · Issue #873 · TokTok/c-toxcore · GitHub	github.com text/html	MISC github.com/TokTok/c-toxcore/issues/873
Security vulnerability and new Toxcore release – Tox Blog	blog.tox.chat text/html	MISC blog.tox.chat/2018/04/security-vulnerability-and-new-toxcore-release
Restrict packet kinds that can be sent through onion path. by kurnevsky · Pull Request #872 · TokTok/c-toxcore · GitHub	github.com text/html	MISC github.com/TokTok/c-toxcore/pull/872

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digitalocean	Toxcore	All	All	All	All
Application	Toktok	Toxcore	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→