



CVE-2019-19794

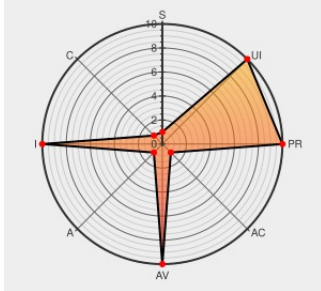
Published on: 12/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19794

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Miekg-dns](#) from [Miekg-dns Project](#) contain the following vulnerability:

The miekg Go DNS package before 1.1.25, as used in CoreDNS before 1.6.6 and other products, improperly generates random numbers because math/rand is used. The TXID becomes predictable, leading to response forgeries.

CVE-2019-19794 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Use crypto/rand for random id generation. by jsha · Pull Request #1044 · miekg/dns · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/miekg/dns/pull/1044

CoreDNS 1.6.6 Release Tracking · Issue #3519 · coredns/coredns · GitHub

Issue Tracking

Third Party Advisory

github.com

text/html

MISC
github.com/coredns/coredns/issues/3519

[security] Predictable TXID can lead to response forgeries · Issue #1043 · miekg/dns · GitHub

Exploit

Issue Tracking

Third Party Advisory

github.com

text/html

MISC
github.com/miekg/dns/issues/1043

[Security] CVE-2019-19794 · Issue #3547 · coredns/coredns · GitHub

Third Party Advisory

github.com

text/html

CONFIRM
github.com/coredns/coredns/issues/3547

Comparing v1.1.24...v1.1.25 · miekg/dns · GitHub

Release Notes

Third Party Advisory

github.com

text/html

MISC
github.com/miekg/dns/compare/v1.1.24...v1.1.25

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

982542 Go (go) Security Update for github.com/miekg/dns (GHSA-44r7-7p62-q3fr)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Miekg-dns Project	Miekg-dns	All	All	All	All
Application	Miekg-dns Project	Miekg-dns	All	All	All	All
cpe:2.3:a:miekg-dns_project:miekg-dns:*.***.***.***						
cpe:2.3:a:miekg-dns_project:miekg-dns:*.***.***.***						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →