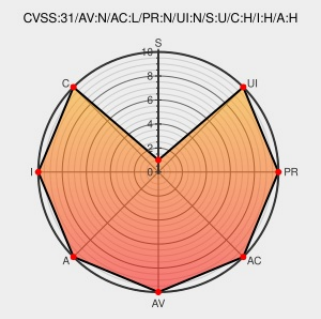
CVE-2020-36363

Published on: 08/12/2021 12:00:00 AM UTC

Last Modified on: 08/23/2021 04:46:00 PM UTC

CVE-2020-36363

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



Certain versions of Amazon Cloudfront from Amazon contain the following vulnerability:

Amazon AWS CloudFront TLSv1.2_2019 allows TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, which some entities consider to be weak ciphers.

CVE-2020-36363 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
amazon web services - Is it possible to disable some specific ciphers from CloudFront? - Stack Overflow	stackoverflow.com text/html	MISC stackoverflow.com/questions/62071604
Amazon CloudFront announces new TLS1.2 security policy for viewer connections	aws.amazon.com text/html	MISC aws.amazon.com/about-aws/whats-new/2020/07/cloudfront-tls-security-policy/

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	Amazon	Amazon Cloudfront	1.2_2019	All	All	All

cpe:2.3:a:amazon:amazon_cloudfront:1.2_2019:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-36363 : Amazon AWS CloudFront TLSv1.2_2019 allows TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 and TLS_ECDHE_RSA_… twitter.com/i/web/status/1…	2021-08-12 22:05:35

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report