



CVE-2021-32827

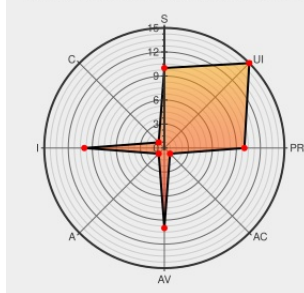
Published on: 08/16/2021 12:00:00 AM UTC

Last Modified on: 07/02/2022 06:21:00 PM UTC

CVE-2021-32827 - advisory for GHSL-2021-059

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

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



Certain versions of [Mockserver](#) from [Mock-server](#) contain the following vulnerability:

MockServer is open source software which enables easy mocking of any system you integrate with via HTTP or HTTPS. An attacker that can trick a victim into visiting a malicious site while running MockServer locally, will be able to run arbitrary code on the MockServer machine.

With an overly broad default CORS configuration MockServer allows any site to send cross-site requests. Additionally, MockServer allows you to create dynamic expectations using Javascript or Velocity templates. Both engines may allow an attacker to execute arbitrary code on-behalf of MockServer. By combining these two issues (Overly broad CORS configuration + Script injection), an attacker could serve a malicious page so that if a developer running MockServer visits it, they will get compromised. For more details including a PoC see the referenced GHSL-2021-059.

CVE-2021-32827 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [mock-server](#) - **mockserver** version **all**

CVSS3 Score: **9.6 - CRITICAL**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	Integrity	Availability

Confidentiality Impact

Partial

Integrity Impact

Partial

Availability Impact

Partial

CVE References

Description	Tags	Link
GHSL-2021-059: Arbitrary code execution in MockServer - CVE-2021-32827 GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2021-059-mockserver/
Oracle Critical Patch Update Advisory - January 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujan2022.html

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

981431 Java (maven) Security Update for org.mock-server:mockserver (GHSA-v3cg-h3f6-2242)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mock-server	Mockserver	All	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.14.0	All	All	All

cpe:2.3:a:mock-server:mockserver:*****:

cpe:2.3:a:oracle:communications_cloud_native_core_policy:1.14.0:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GHSecurityLab	GHSL-2021-059: Arbitrary code execution in MockServer - CVE-2021-32827 github.co/36P4D8W	2021-07-21 19:10:01
@CVEreport	CVE-2021-32827 : MockServer is open source software which enables easy mocking of any system you integrate with via... twitter.com/i/web/status/1...	2021-08-16 20:56:31
@LinInfoSec	Velocity - CVE-2021-32827: securitylab.github.com/advisories/GHS...	2021-08-16 22:25:38

[← Previous ID](#)

[Next ID →](#)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)