



# CVE-2021-22540

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-22540
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-22 15:15:00 UTC
<b>Updated</b>	2021-04-26 20:20:00 UTC
<b>Description</b>	Bad validation logic in the Dart SDK versions prior to 2.12.3 allow an attacker to use an XSS attack via DOM clobbering. Th

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dart	Dart Software Development Kit	All	All	All	All

## References

Reference	Source	Link	Tags
[dart:html] Fix sanitization for HTML templates · dart-lang/sdk@ce5a1c2 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>	
<a href="https://github.com/dart-lang/sdk/security/advisories/GHSA-3rfv-4jvg-9522">github.com/dart-lang/sdk/security/advisories/GHSA-3rfv-4jvg-9522</a>	CONFIRM	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Vincenzo di Cicco

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

**Free CVE JSON API** [cve.report/api](#)

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