

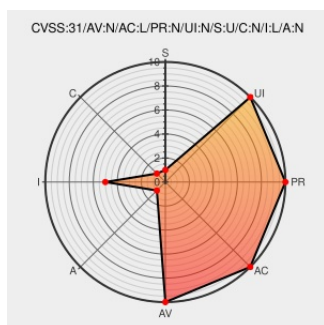


CVE-2020-36563

Published on: Not Yet Published

Last Modified on: 02/28/2023 06:07:15 PM UTC

CVE-2020-36563

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

Certain versions of [Go-saml](#) from [Robotsandpencils](#) contain the following vulnerability:

XML Digital Signatures generated and validated using this package use SHA-1, which may allow an attacker to craft inputs which cause hash collisions depending on their control over the input.

CVE-2020-36563 has been assigned by [security@golang.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [github.com/RobotsAndPencils/go-saml](#) - [github.com/RobotsAndPencils/go-saml](#) version **not down converted**

CVSS3 Score: **5.3 - MEDIUM**

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

CVE References

Description	Tags	Link
GO-2020-0047 - Go Packages	pkg.go.dev text/html	MISC pkg.go.dev/vuln/GO-2020-0047
sign AuthnRequests and AuthnResponses with SHA256 by mattg-sigsci · Pull Request #38 · RobotsAndPencils/go-saml · GitHub	github.com text/html	MISC github.com/RobotsAndPencils/go-saml/pull/38

By selecting these links, you may be leaving CVEreport workspace. 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

Exploit/POC from Github

XML Digital Signatures generated and validated using this package use SHA-1, which may allow an attacker to craft inp...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Robotsandpencils	Go-saml	-	All	All	All
cpe:2.3:a:robotsandpencils:go-saml:-:*:*:*:go:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-36563 : XML Digital Signatures generated and validated using this package use SHA-1, which may allow an at... twitter.com/i/web/status/1...	2022-12-28 03:02:23
 /r/netcve	CVE-2020-36563	2022-12-28 04:38:55

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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