



CVE-2021-22565

Published on: 12/09/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 04:20:00 PM UTC

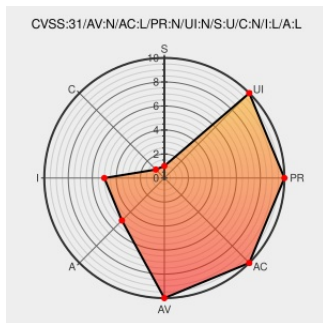
CVE-2021-22565

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Exposure Notification Verification Server](#) from [Google](#) contain the following vulnerability:

An attacker could prematurely expire a verification code, making it unusable by the patient, making the patient unable to upload their TEKs to generate exposure notifications. We recommend upgrading the Exposure Notification server to V1.1.2 or greater.

CVE-2021-22565 has been assigned by security@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: Google LLC - Google Exposure-notifications-verification-server version < 1.1.2

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Release v1.1.2 · google/exposure-notifications-verification-server · GitHub	github.com text/html	MISC github.com/google/exposure-notifications-verification-server/releases/tag/v1.1.2

Insufficient Granularity of Access Control in github.com/google/exposure-notifications-verification-server · Advisory · google/exposure-notifications-verification-server · GitHub

github.com
text/html

MISC github.com/google/exposure-notifications-verification-server/security/advisories/GHSA-wx8q-rgfr-cf6v

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

980123 Go (go) Security Update for github.com/google/exposure-notifications-verification-server (GHSA-wx8q-rgfr-cf6v)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Exposure Notification Verification Server	All	All	All	All
cpe:2.3:a:google:exposure_notification_verification_server:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-22565 : An attacker could prematurely expire a verification code, making it unusable by the patient, makin... twitter.com/i/web/status/1...	2021-12-09 12:56:41
 /r/netcve	CVE-2021-22565	2021-12-09 14:38:27

← 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](#)