

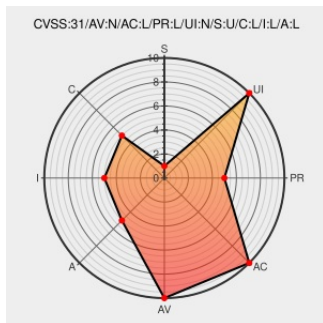


CVE-2021-22538

Published on: 03/31/2021 12:00:00 AM UTC

Last Modified on: 04/06/2021 02:11:00 PM UTC

CVE-2021-22538

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

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

A privilege escalation vulnerability impacting the Google Exposure Notification Verification Server (versions prior to 0.23.1), allows an attacker who (1) has UserWrite permissions and (2) is using a carefully crafted request or malicious proxy, to create another user with higher privileges than their own. This occurs due to insufficient checks on the allowed set of permissions. The new user creation event would be captured in the Event Log.

CVE-2021-22538 has been assigned by [Google](#) security@google.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Google](#) **Google LLC - Exposure Notifications Verification Server** version **<= 0.23.0**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Release v0.24.0 · google/exposure-notifications-verification-server · GitHub

github.com
text/html

CONFIRM github.com/google/exposure-notifications-verification-server/releases/tag/v0.24.0

Privilege escalation in rbac · Advisory · google/exposure-notifications-verification-server · GitHub

github.com
text/html

CONFIRM github.com/google/exposure-notifications-verification-server/security/advisories/GHSA-5v95-v8c8-3rh6

Release v0.23.1 · google/exposure-notifications-verification-server · GitHub

github.com
text/html

CONFIRM github.com/google/exposure-notifications-verification-server/releases/tag/v0.23.1

Merge pull request from GHSA-5v95-v8c8-3rh6 · google/exposure-notifications-verification-server@eb8cf40 · GitHub

github.com
text/html

CONFIRM github.com/google/exposure-notifications-verification-server/commit/eb8cf40b12dbe79304f1133c06fb73419383cd95

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

982434 Go (go) Security Update for github.com/google/exposure-notifications-verification-server (GHSA-5v95-v8c8-3rh6)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Exposure Notifications Verification Server	All	All	All	All
cpe:2.3:a:google:exposure_notifications_verification_server:*****:						

Discovery Credit

Michael Mazzolini (Ethical Hacker at WHO)

Social Mentions		
Source	Title	Posted (UTC)
📧 @CVEreport	CVE-2021-22538 : A privilege escalation vulnerability impacting the Google Exposure Notification Verification Serve... twitter.com/i/web/status/1...	2021-03-31 21:17:09