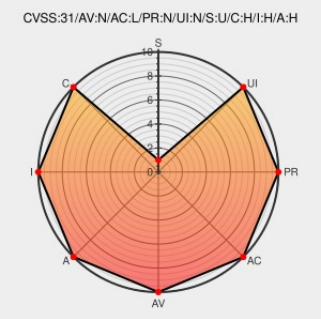
CVE-2023-30845

Published on: Not Yet Published

Last Modified on: 05/09/2023 04:08:00 PM UTC

CVE-2023-30845 - advisory for GHSA-6qmp-9p95-fc5f

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Espv2 from Google contain the following vulnerability:

ESPv2 is a service proxy that provides API management capabilities using Google Service Infrastructure. ESPv2 2.20.0 through 2.42.0 contains an authentication bypass vulnerability. API clients can craft a malicious `X-HTTP-Method-Override` header value to bypass JWT authentication in specific cases. ESPv2 allows malicious requests to bypass authentication if both the conditions are true: The requested HTTP method is **not** in the API service definition (OpenAPI spec or gRPC `google.api.http` proto annotations, and the specified `X-HTTP-Method-Override` is a valid HTTP method in the API service definition. ESPv2 will forward the request to your backend without checking the JWT. Attackers can craft requests with a malicious `X-HTTP-Method-Override` value that allows them to bypass specifying JWTs. Restricting API access with API keys works as intended and is not affected by this vulnerability. Upgrade deployments to release v2.43.0 or higher to receive a patch. This release ensures that JWT authentication occurs, even when the caller specifies `x-http-method-override`. `x-http-method-override` is still supported by v2.43.0+. API clients can continue sending this header to ESPv2.

CVE-2023-30845 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **GoogleCloudPlatform** - **esp-v2** version **= >= 2.20.0, < 2.43.0**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
Add back in HTTP method override in service control filter (#802) · GoogleCloudPlatform/esp-v2@e98061e · GitHub	github.com text/html	MISC github.com/GoogleCloudPlatform/esp-v2/commit/e98061ee4527a564506ba4e814c0ecf324dc2c6f
move x-http-method-override to beginning of filter chain (#801) · GoogleCloudPlatform/esp-v2@e956701 · GitHub	github.com text/html	MISC github.com/GoogleCloudPlatform/esp-v2/commit/e95670146f5e96bb5565b0a9c1e153886b3e04ce
Changelog for v2.43.0 · GoogleCloudPlatform/esp-v2@0bcdfc0 · GitHub	github.com text/html	MISC github.com/GoogleCloudPlatform/esp-v2/commit/0bcdfc024ce96b34db4e1b4f2211b509d9be93cd
JWT authentication bypass via `X-HTTP-Method-Override` header · Advisory · GoogleCloudPlatform/esp-v2 · GitHub	github.com text/html	MISC github.com/GoogleCloudPlatform/esp-v2/security/advisories/GHSA-6qmp-9p95-fc5f

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Espv2	All	All	All	All

cpe:2.3:a:google:espv2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-30845 : ESPv2 is a service proxy that provides API management capabilities using Google Service Infrastruc… twitter.com/i/web/status/1…	2023-04-26 21:06:53
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-30845 ESPv2 is a service proxy that provides API management capabilitie… twitter.com/i/web/status/1…	2023-04-26 22:10:58

← 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 registred 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