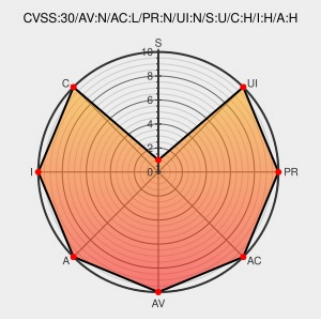
CVE-2017-18365

Published on: 03/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18365

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



Certain versions of Github from Github contain the following vulnerability:

The Management Console in GitHub Enterprise 2.8.x before 2.8.7 has a deserialization issue that allows unauthenticated remote attackers to execute arbitrary code. This occurs because the enterprise session secret is always the same, and can be found in the product's source code. By sending a crafted cookie signed with this secret, one can call Marshal.load with arbitrary data, which is a problem because the Marshal data format allows Ruby objects.

CVE-2017-18365 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
GitHub Enterprise Remote Code Execution	Exploit	MISC www.exablue.de/blog/2017-03-15-github-enterprise

GitHub Enterprise Remote Code Execution	Exploit Third Party Advisory www.exablue.de text/html	MISC www.exablue.de/blog/2017-03-15-github-enterprise-remote-code-execution.html
GitHub Enterprise - The best way to build and ship software	Vendor Advisory enterprise.github.com text/html	MISC enterprise.github.com/releases/2.8.7/notes

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	Github	Github	All	All	All	All
Application	Github	Github	2.8.7	All	All	All
Application	Github	Github	All	All	All	All
Application	Github	Github	2.8.7	All	All	All

cpe:2.3:a:github:github:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:github:github:2.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:github:github:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:github:github:2.8.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→