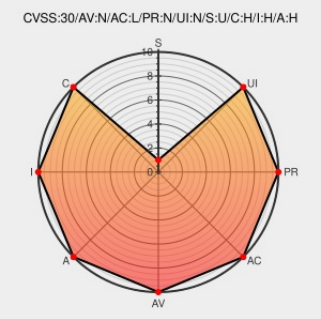
CVE-2018-10362

Published on: 04/25/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-10362

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



Certain versions of Phpliteadmin from Phpliteadmin contain the following vulnerability:

An issue was discovered in phpLiteAdmin 1.9.5 through 1.9.7.1. Due to loose comparison with '==' instead of '===' in classes/Authorization.php for the user-provided login password, it is possible to login with a simpler password if the password has the form of a power in scientific notation (like '2e2' for '200' or '0e1234' for '0'). This is possible because, in the loose comparison case, PHP interprets the string as a number in scientific notation, and thus converts it to a number. After that, the comparison with '==' casts the user input (e.g., the string '200' or '0') to a number, too. Hence the attacker can login with just a '0' or a simple number he has to brute force. Strong comparison with '===' prevents the cast into numbers.

CVE-2018-10362 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: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Authorization bypass in Authorization.php · Issue #11 · phpLiteAdmin/pla · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/phpLiteAdmin/pla/issues/11
Site not found · GitHub Pages	Technical Description Third Party Advisory k3research.outerhaven.de text/html Inactive Link Not Archived	MISC k3research.outerhaven.de/posts/small-mistakes-lead-to-big-problems.html

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	Phpliteadmin	Phpliteadmin	All	All	All	All

cpe:2.3:a:phpliteadmin:phpliteadmin:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→