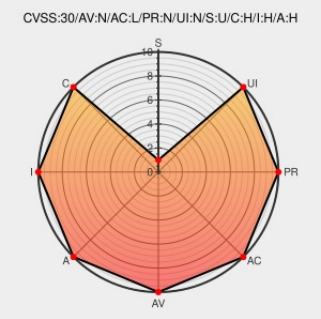
CVE-2018-3810

Published on: 01/01/2018 12:00:00 AM UTC

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

CVE-2018-3810

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



Certain versions of Smart Google Code Inserter from Oturia contain the following vulnerability:

Authentication Bypass vulnerability in the Oturia Smart Google Code Inserter plugin before 3.5 for WordPress allows unauthenticated attackers to insert arbitrary JavaScript or HTML code (via the sgcgoogleanalytic parameter) that runs on all pages served by WordPress. The saveGoogleCode() function in smartgooglecode.php does not check if the current request is made by an authorized user, thus allowing any unauthenticated user to successfully update the inserted code.

CVE-2018-3810 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
Smart Google Code Inserter – WordPress plugin | WordPress.org	Release Notes	MISC

Smart Google Code Inserter – WordPress plugin | WordPress.org	Release Notes Third Party Advisory wordpress.org text/html	MISC wordpress.org/plugins/smart-google-code-inserter/#developers
Smart Google Code Inserter <= 3.4 - Unauthenticated Cross-Site Scripting (XSS)	Third Party Advisory VDB Entry web.archive.org text/html Inactive Link Not Archived	MISC wpvulndb.com/vulnerabilities/8987
Smart Google Code Inserter < 3.5 - Auth Bypass/SQLi	Exploit Third Party Advisory limbenjamin.com text/html	MISC limbenjamin.com/articles/smart-google-code-inserter-auth-bypass.html
WordPress Plugin Smart Google Code Inserter < 3.5 - Authentication Bypass / SQL Injection - PHP webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43420

There are currently no QIDs associated with this CVE

Exploit/POC from Github

cve-2018-3810

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oturia	Smart Google Code Inserter	All	All	All	All
Application	Oturia	Smart Google Code Inserter	All	All	All	All

cpe:2.3:a:oturia:smart_google_code_inserter:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:oturia:smart_google_code_inserter:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report