tenable

SQL Injection in SRS Simple Hits Counter Plugin for WordPress

Medium

← View More Research Advisories

Synopsis

Tenable has discovered a blind SQL injection vulnerability in the SRS Simple Hits Counter plugin for WordPress due to improper validation of user supplied input data. The root cause of the issue occurs in the srs_simple_hits_counter function which fails to validate the contents of the post_id variable. This variable value is used to form an SQL query in the update_views_visitors function.

An unauthenticated, remote attacker can exploit this issue via crafted requests to disclose potentially sensitive information from the WordPress database (e.g. admin password hash). We have verified this vulnerability is present when installed on Ubuntu Linux x64 and Windows x64.

For example:

In srs_simple_hits_counter, the post_id variable is set as such:

```
$post_id = $_GET['post_id'];
```

And then in update_views_visitors, a SQL query is constructed with this value:

```
$post_data = $wpdb->get_results("SELECT * FROM $table_name WHERE (srs_post_id = $post_id AND srs_date = '".$date."' )");
```

Proof of Concept

The PoC will attempt to exploit this issue to retrieve the admin password hash from the WordPress database by sending multiple specially crafted requests. The following is an example of how to use the PoC:

```
python3 blind_sqli_tra_2020_42.py http://192.168.1.195/wordpress
```

Solution

Upgrade to version 1.1.0

Additional References

https://wordpress.org/plugins/srs-simple-hits-counter/
https://github.com/tenable/poc/blob/master/WordPress/plugins/SRS_Simple_Hits_Counter/blind_sqli_tra_2020_42.py

Disclosure Timeline

06/09/2020 - Tenable attempts to contact the developer directly. Email bounced back.
06/10/2020 - Reported vulnerability to Wordpress plugin team. 90-day date set to September 08, 2020.
06/11/2020 - Automated response from WordPress plugin team.
06/30/2020 - Tenable asks for an update.
07/01/2020 - WordPress plugin team replies with no update.
07/09/2020 - Tenable notices a fix in the plugin. Notifies WordPress that we will be releasing an advisory, and also that the fix is incomplete. Asks if WP will request CVE.
07/10/2020 - WordPress will not request CVE. Says we can.

Risk Information

CVE ID: CVE-2020-5766
Tenable Advisory ID: TRA-2020-42
Credit: Alex Peña

CVSSv2 Base / Temporal Score: 5.0
CVSSv2 Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Affected Products: 1.0.3, 1.0.4
Risk Factor: Medium

Advisory Timeline

07/10/2020 - Advisory published.
07/21/2020 - Updated solution.

tenable

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media

tenable

Privacy Policy Legal 508 Compliance