Unauthenticated email forgery/spoofing in WordPress Email Subscribers plugin

High

← View More Research Advisories

Synopsis

WordPress Email Subscribers & Newsletters plugin by Icegram prior to version 4.5.6 is affected by an unauthenticated email forgery/spoofing vulnerability in the **class-es-newsletters.php** class. It allows a remote unauthenticated attacker to send forged emails to all recipients from the available lists of contacts or subscribers, with complete control over the content and subject of the email. This is done via a crafted ajax request which tricks the application into creating a new broadcast and schedules a greeting email with the content modified that gets sent after about a minute or so. PoC Request:

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 172.16.68.178
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 222

action=admin_init&broadcast_data[id]=999&ig_es_broadcast_submitted=submitted&broadcast_data[subject]=test999&broadcast_data[body]=body-content&broadcast_data[list_ids]=2&broadca
```

Solution

Upgrade to WordPress Email Subscribers & Newsletters plugin by Icegram version 4.5.6 or higher.

Disclosure Timeline

8/26/2020 - Disclosure Email sent. 90 day date, November 24th.
8/31/2020 - Follow up email sent.
9/6/2020 - Vendor Acknowledges
9/8/2020 - Tenable asks for patch date
9/9/2020 - Vendor releases patches

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2020-5780
Tenable Advisory ID: TRA-2020-53
Credit: Alex Peña

CVSSv3 Base / Temporal Score: 7.5 / 6.7
CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Affected Products: WordPress Email Subscribers & Newsletters plugin by Icegram prior to version 4.5.6.
Risk Factor: High

Advisory Timeline

09/09/2020 - Advisory published.

→ 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