Security release for all versions of Mautic prior to 2.16.5 and 3.2.4

mautibot Jan '21

We have made available for immediate download an out-of-sequence release for both Mautic 2.x and 3.x.

⚠ Important note for users who are currently running 3.2.0 or later

Are you currently using Mautic 3.2.0 or later **and do you update through the CLI (Command Line Interface)**? Then the message below applies to you! This **does not apply** if you're updating through the UI (graphical interface).

When you're trying to update through the CLI, you might run into the following error:

```
Notice: Undefined index: message in /var/www/html/app/bundles/CoreBundle/U

Failed to execute command php bin/console mautic:update:apply: exit statu
```

This bug was introduced in Mautic 3.2.0 and fixed in 3.2.4. Please use the following workaround:

```
wget https://github.com/mautic/mautic/releases/download/3.2.4/3.2.4-update
php bin/console mautic:update:apply --update-package=3.2.4-update.zip
php bin/console mautic:update:apply --finish
```

We have also published some resources on the website:

- Landing page for the security team
- Security Advisory Policy
- How to report a security issue
- How we triage, resolve and release fixes for security issues
- How to join the Mautic Security Team
- Meet the Mautic Security Team

This release addresses:

1. A **Moderately Critical** Vulnerability (Vulnerability 1) reported by Dardan Prebreza at Bishop Fox, and
2. A **Highly Critical** Vulnerability (Vulnerability 2) reported by Naveen Sunkavally at Horizon3.ai.

Risk Ratings

These are based on the information in the 'how we triage, resolve and release fixes for security issues ' page above.

Vulnerability 1

12/25 (**Moderately Critical**) AC:Complex/A:Admin/CI:Some/II:Some/E:Theoretical/TD:All

Vulnerability 2

22/25 (**Highly Critical**) AC:None/A:None/CI:All/II:All/E:Theoretical/TD:All

As Vulnerability 2 affects **every released version** of Mautic and allows an attacker to create a user in Mautic with elevated privileges, all users are **strongly urged** to update immediately.

More information can be found in the CVE reports here - details will be added following the release:

Vulnerability 1

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3142

Vulnerability 2

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35124

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35125

Patches

The easiest way to protect your Mautic instances is to simply update to 2.16.5 or 3.2.3 in the usual way. If you are unable to do this for any reason, the patch files are provided below.

Skip to main content

Fix for both vulnerabilities

Link to patch for 2.x versions: **https://github.com/mautic/mautic/compare/2.16.4...2.16.5.diff**

Link to patch for 3.x versions: **https://github.com/mautic/mautic/compare/3.2.2...3.2.3.diff**

How to scan for attempts to exploit the vulnerability

We have also provided some searches that you can do to see if there have been attempts to exploit the highly critical vulnerability.

Check for exploit attempts - Vulnerability 1

To see if there was an attempt at this vulnerability, run the following queries replacing PREFIX_ with your own if configured:

- >select * from PREFIX_companies where companyname like '%<%' or companyname like '%onerror%';

Check for exploit attempts - Vulnerability 2

The first and absolutely necessary step is to check if there are any unrecognized users listed in Mautic’s User manager. Delete or unpublish any not recognized immediately.

To see if there was an attempt at this vulnerability, run the following queries replacing PREFIX_ with your own if configured:

- >select * from PREFIX_form_submissions where referer like '%<%' or referer like '%onerror%';
- >select * from PREFIX_asset_downloads where referer like '%<%' or referer like '%onerror%';
- >select * from PREFIX_companies where companyname like '%<%' or companyname like '%onerror%';

If there are any results returned, review them to look for HTML tags. If it looks like HTML is embedded, delete the entry from the database.

Credits

Thanks to Dardan Prebreza at Bishop Fox and Naveen Sunkavally at Horizon3.ai for responsibly reporting these vulnerabilities.

Thanks to Alan Hartless at Acquia and Dennis Ameling for fixing these vulnerabilities.

This is a companion discussion topic for the original entry at **https://www.mautic.org/blog/community/security-release-all-versions-mautic-prior-2-16-5-and-3-2-3**