Secret data exfiltration via symfony parameters

Moderate **alanhartless** published **GHSA-4hjq-422q-4vpx** on Mar 22, 2021

Package

mautic/core (php)

Affected versions	Patched versions
< 3.3.2	3.3.2

Description

Impact

Symfony parameters (which is what Mautic transforms configuration parameters into) can be used within other Symfony parameters by design. However, this also means that an admin who is normally not privy to certain parameters, such as database credentials, could expose them by leveraging any of the free text fields in Mautic's configuration that are used in publicly facing parts of the application.

For example,

1. Go to Configuration page -> Landing Page Settings -> Analytics script and enter this: `< script> console.log("db password is: %mautic.db_password%"); </script>`
2. Visit any landing page and open the JS dev console. You will see the following message with real instance db password: `db password is: <real password>`

Risk rating: ModerateCVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L

Patches

Upgrade to 3.3.2

Workarounds

No

References

No

For more information

If you have any questions or comments about this advisory:

- Email us at security@mautic.org

Severity

Moderate 5.8 / 10

CVSS base metrics

Attack vector	Local
Attack complexity	High
Privileges required	High
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	Low

CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L

CVE ID

CVE-2021-27908

Weaknesses

CWE-200

Credits

Gregy

fedys