Sensitive Information Disclosure in extension "Media Content Element" (mediace)

Critical **bmack** published **GHSA-4h44-w6fm-548g** on Jul 28, 2020

Package

php **friendsoftypo3/mediace** (Composer)

Affected versions	Patched versions
>= 7.6.2, <= 7.6.4	7.6.5

Description

Meta

- CVSS: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C` (9.1)
- CWE-325, CWE-20, CWE-200, CWE-502

Problem

It has been discovered that an internal verification mechanism can be used to generate arbitrary checksums. This allows to inject arbitrary data having a valid cryptographic message authentication code (HMAC-SHA1) and can lead to various attack chains as described below.

- TYPO3-CORE-SA-2020-007, CVE-2020-15099: Potential Privilege Escalation
  - the database server used for a TYPO3 installation must be accessible for an attacker (either via internet or shared hosting network)
  - `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C` (7.5, high)
- TYPO3-CORE-SA-2016-013, CVE-2016-5091: Insecure Deserialization & Remote Code Execution
  - an attacker must have access to at least one Extbase plugin or module action in a TYPO3 installation
  - `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C` (9.1, critical)

The overall severity of this vulnerability is critical (9.1) based on mentioned attack chains and the fact it does not require any privileges.

Solution

In case the extension is not used and required at all, it is suggested to uninstall and remove it from the system completely. Otherwise, an updated version 7.6.5 is available from the TYPO3 extension manager, Packagist and the TYPO3 extension repository:

- https://extensions.typo3.org/extension/download/mediace/7.6.5/zip/
- https://packagist.org/packages/friendsoftypo3/mediace#7.6.5

As a precautionary measure it is advised to change `encryptionKey` and database credentials in `typo3conf/LocalConfiguration.php`.

Credits

Thanks to TYPO3 security team member Oliver Hader who reported and fixed the issue.

References

- TYPO3-EXT-SA-2020-014

Severity

Critical

CVE ID

CVE-2020-15086

Weaknesses

No CWEs

Credits

ohader