mybb / mybb Public

Code Issues 244 Pull requests 48 Actions Projects 3 Wiki ···

Nested Email MyCode Persistent XSS

High **dvz** published **GHSA-6483-hcpp-p75w** on Feb 22, 2021

Package

MyBB

Affected versions	Patched versions
< 1.8.25	1.8.25

Description

Impact

The parsing of messages containing unexpectedly nested `[email]` MyCode (BBCode) tags may result in malformed HTML output, leading to an XSS vulnerability.

The vulnerability can be exploited with minimal user interaction by pointing a victim to page where a maliciously crafted MyCode message is rendered. This may occur when:

- a new message form with instant preview is pre-filled through a POST or GET parameter, or
- a message previously saved on the server (e.g. as a post or Private Message) is displayed.

The impact may be reduced when:

- the `[email]` MyCode is disabled (*Admin CP → Configuration → Settings → Clickable Smilies and BB Code*: *Allow Email MyCode* setting is set to *Off*), or
- MyCode is disabled for individual forums, Private Messages, user profile signatures, and calendars, or
- guest users are not allowed to submit messages where MyCode is supported, or posting access is otherwise limited or controlled.

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

Overview

The HTML output of the `[email]` MyCode may include opening `[` and closing `]` square brackets in the value of the `href=""` attribute of the `<a>` tag.
This may result in unexpected, further parsing of MyCode and insertion of output in the parameter value with unescaped, colliding quotation marks `"`, leading to an XSS vulnerability.

Patches

MyBB 1.8.25 resolves this issue with the following changes:

- Commit: `cb781b4`
  - `.patch` : https://github.com/mybb/mybb/commit/cb781b49116bf5c4d8deca3e17498122b701677a.patch

Workarounds

To reduce impact without upgrading MyBB, change the following setting (*Admin CP → Configuration → Settings*):

- *Clickable Smilies and BB Code → Allow Email MyCode*: *Off*

References

- Release Notes: https://mybb.com/versions/1.8.25/

For more information

Go to mybb.com/security to report possible security concerns or to learn more about security research at MyBB.

Contact

The security team can be reached at security@mybb.com.

Severity

High

CVE ID

CVE-2021-27279

Weaknesses

CWE-79