



# CVE-2016-15032

Published on: Not Yet Published

Last Modified on: 10/20/2023 12:15:00 PM UTC

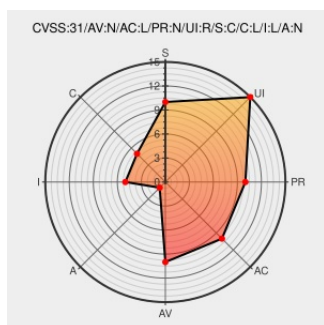
## CVE-2016-15032

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Mh Httpbl](#) from [Mh Httpbl Project](#) contain the following vulnerability:

**\*\* UNSUPPORTED WHEN ASSIGNED \*\* \*\* UNSUPPORTED WHEN ASSIGNED \*\*** A vulnerability classified as problematic has been found in mback2k mh\_httpbl Extension up to 1.1.7 on TYPO3. This affects the function stopOutput of the file class.tx\_mhhttpbl.php. The manipulation of the argument `$_SERVER['REMOTE_ADDR']` leads to

cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.1.8 is able to address this issue. The patch is named `a754bf306a433a8c18b55e25595593e8f19b9463`. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-230391. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2016-15032 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |

## CVE References

| Description                                                       | Tags                                                                                               | Link                                         |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------------------------------------|
| Login required                                                    | <a href="#">vuldb.com</a><br><a href="#">text/html</a><br><b>Inactive Link</b> <b>Not Archived</b> | <a href="#">MISC vuldb.com/?ctiid.230391</a> |
| CVE-2016-15032: mback2k mh_httpbl Extension class.tx_mhhttpbl.php | <a href="#">vuldb.com</a><br><a href="#">text/html</a>                                             | <a href="#">MISC vuldb.com/?id.230391</a>    |

stopOutput cross site scripting

Fix possible Cross-Site Scripting by escaping remote addr and host · mback2k/mh\_httpbl@a754bf3 · GitHub

github.com  
text/html

MISC

github.com/mback2k/mh\_httpbl/commit/a754bf306a433a8c18b55e25595593e8f1

Release mh\_httpbl\_1.1.8\_security: TYPO3 Security Team: Security Fix PLEASE UPDATE · mback2k/mh\_httpbl · GitHub

github.com  
text/html

MISC

github.com/mback2k/mh\_httpbl/releases/tag/mh\_httpbl\_1.1.8\_security

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type        | Vendor            | Product   | Version | Update | Edition | Language |
|-------------|-------------------|-----------|---------|--------|---------|----------|
| Application | Mh Httpbl Project | Mh Httpbl | All     | All    | All     | All      |

cpe:2.3:a:mh\_httpbl\_project:mh\_httpbl:\*:\*:\*:\*:typo3:\*:\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →