

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

11/06/2015

SUBJECT:

A Vulnerability in vBulletin Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in vBulletin that could allow for remote code execution. vBulletin is a commercial forum and blog platform. Successful exploitation could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and the ability to bypass the security system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

Reports indicate that this vulnerability is being actively exploited in the wild.

SYSTEMS AFFECTED:

- vBulletin 5.1.4 to 5.1.9

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:

A vulnerability has been discovered in vBulletin that could allow for remote code execution. An object injection vulnerability exists in the 'unserialize' call found in the 'vB_Api_Hook::decodeArguments()' method in vBulletin versions 5.1.4 to 5.1.9. This may allow an unauthenticated attacker to submit a request containing a specially crafted '\$argument' in the 'unserialize' call.

Successful exploitation may render the server inoperable, cause permanent data loss, or result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and the ability to bypass the security system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Verify no unauthorized system changes occurred on system before applying patch.
- Apply appropriate updates provided by vBulletin to vulnerable systems immediately after appropriate testing.
- Reset passwords for all users accounts in vBulletin systems

REFERENCES:**vBulletin:**

http://www.vbulletin.com/forum/forum/vbulletin-announcements/vbulletin-announcements_aa/4332166-security-patch-release-for-vbulletin-5-connect-versions-5-1-4-through-5-1-9

Check Point:

<http://blog.checkpoint.com/2015/11/05/check-point-discovers-critical-vbulletin-0-day/>

Pastie:

<http://pastie.org/pastes/10527766/text?key=wq1hgkci4afb9ipqzllsq>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>