



Advisory Alert

Alert No : AAA190117

Date : 19-Jan-17 13:23 PM



Security Updates for 19th January 2017

Overview

High	Openssh	▪ Remote Codes Execution
	Php	▪ Denial of service
	Php	▪ Remote Codes Execution
Medium	Wordpress	▪ Cross-site scripting
	and Wordpress	▪ Directory traversal
Low	IBM	▪ Bypass security constraint

Description / Impact

- Openssh
 - A vulnerability in the OpenSSH before 7.4 allows remote attackers to execute arbitrary code.
- Php
 - A vulnerability in the PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 allows remote attackers to cause a denial of service attack.
- Php
 - A vulnerability in the all versions of PHP 7 allow remote attackers to execute arbitrary codes.
- Wordpress
 - A vulnerability in the WordPress before 4.6.1 might allow remote attackers to inject arbitrary web script or HTML script.
- Wordpress
 - A vulnerability in the WordPress before 4.6.1 allows remote authenticated users to access arbitrary files via Directory traversal attack.
- IBM
 - A vulnerability in the IBM WebSphere Application Server 8.5.x allow attackers to bypass the security constraint.

Risk Reduction Recommendations

Visit the links below and follow the instructions given by respective vendors.

- Openssh <https://packetstormsecurity.com/files/140261/OpenSSH-Arbitrary-Library-Loading.html>
- Php <http://www.php.net/ChangeLog-5.php>
- Php <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7479>
- Wordpress <http://www.openwall.com/lists/oss-security/2016/09/08/19>
- Wordpress https://codex.wordpress.org/Version_4.6.1
- IBM <https://pivotal.io/security/cve-2016-9879>

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.