TLP: WHITE

Advisory Alert

Alert Number : AAA20201013 **Date :** October 13, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
phpMyAdmin	**Medium**	Multiple Vulnerabilities
Apache	**Medium**	Sensitive Data Exposure

Description

Affected Product	phpMyAdmin
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-26934, CVE-2020-26935)
Description	CVE-2020-26934: Vulnerability was discovered in phpMyAdmin wheran attacker can abuse the transformation feature and perform an XSS attack. This is done by sending a crafted link to the victim with the malicious JavaScript. And once the victim clicks on the link the JavaScript will run and execute the instructions by the attacker. It is recommended to apply this patch to avoid in such issues. CVE-2020-26935: SQL injection vulnerability found in phpMyAdmin SearchController allows an attacker to use this flaw to inject malicious SQL in to a query. It is recommended to apply this patch to avoid in such issues.
Affected Products	PhpMyAdmin 5.0.x releases prior to 5.0.3 PhpMyAdmin 4.9.x releases prior to 4.9.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.phpmyadmin.net/security/PMASA-2020-6/ https://www.phpmyadmin.net/security/PMASA-2020-5/

Affected Product	Apache
Severity	**Medium**
Affected Vulnerability	Sensitive Data Exposure (CVE-2020-13943)
Description	Vulnerability in Apache leads to users seeing responses for unexpected resources. This happens when an HTTP/2 client which connects to Apache Tomcat exceeds the maximum number of concurrent streams for a connection. Due to this flaw there is a possibility of the existence of previously requested HTTP headers – including HTTP/2 pseudo headers in the request rather than the intended headers.
Affected Products	Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	http://tomcat.apache.org/security-10.html http://tomcat.apache.org/security-9.html http://tomcat.apache.org/security-8.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.