Advisory Alert

Alert Number: AAA20201102 **Date:** November 2, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PHP	**High**	Security Patch Updates
Samba	**Medium**	Multiple Vulnerabilities

Description

Affected Product	PHP
Severity	**High**
Affected Vulnerability	Security Patch Updates
Description	PHP has released updates addressing security bug fixes that exist in PHP. It is highly recommended to apply necessary fixes provided on the official PHP website at the earliest to avoid these security issues and all PHP 7.4 and 7.3 users are encouraged to upgrade 7.4.12 and 7.3.24
Affected Products	PHP 7.4 PHP 7.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/archive/2020.php#2020-10-29-3 https://www.php.net/archive/2020.php#2020-10-29-1 https://www.php.net/ChangeLog-7.php#PHP_7_3 https://www.php.net/ChangeLog-7.php#PHP_7_4

Affected Product	Samba
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-14318), (CVE-2020-14323), (CVE-2020-14383)
Description	**CVE-2020-14318** - The SMB 1, 2 and 3 protocols client can request file name notification on a directory handle when a condition such as new file creation or file size change or file timestamp update error occurs **CVE-2020-14323** - It was an obvious extension to also offer this batch operation on the winbind unix domain connectivity to local processes on the Samba server to reduce network traffic to the domain controller **CVE-2020-14383** - Samba's dnsserver RPC pipe made an error in handling the case there are no records present instead of noticing the lack of records, it dereferenced uninitialized memory, causing the RPC server to crash
Affected Products	Samba 3.6.0 Samba 4.0 and later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2020-14318.html https://www.samba.org/samba/security/CVE-2020-14323.html https://www.samba.org/samba/security/CVE-2020-14383.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.