Advisory Alert

Alert Number: AAA20241122 **Date:** November 22, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PHP	**High**, **Medium**	Multiple Vulnerabilities
FortiGuard	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**PHP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-11233, CVE-2024-11234, CVE-2024-11236, CVE-2024-8929, CVE-2024-8932)
Description	PHP has released security updates addressing multiple vulnerabilities that exist in their products. Malicious users could exploit these vulnerabilities to cause Server Side Request Forgery attacks, Denial of Service, Integer Overflow, SQL code Injection, Out-of-bounds Write. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP 8.4 -Versions Prior to 8.4.1 PHP 8.3 - Versions Prior to 8.3.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/ChangeLog-8.php#8.4.1

Affected Product	**FortiGuard**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27316, CVE-2024-24549, CVE-2024-30255, CVE-2023-45288, CVE-2024-28182, CVE-2024-27983, CVE-2024-3302)
Description	FortiGuard has released security updates addressing Multiple Vulnerabilities that exist in their products. Malicious users could exploit these vulnerabilities to cause Multiple Denial of Service Attacks. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiSandbox 4.4 - Versions 4.4.0 through 4.4.5 FortiSwitch 7.4 - Versions 7.4.0 through 7.4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-120

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.