TLP: WHITE

Advisory Alert

Alert Number: AAA20240610 **Date:** June 10, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PHP	**Critical**	OS Command Injection Vulnerability
NETGEAR	**High**	Post-Authentication Command Injection Vulnerability
PHP	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**PHP**
Severity	**Critical**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2024-4577)
Description	PHP has released security updates addressing an OS Command Injection Vulnerability that exists in their products. This vulnerability exists due to improper input validation in PHP-CGI implementation. A remote attacker can send specially crafted HTTP request to the application and execute arbitrary OS commands on the system. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20 and 8.3.* before 8.3.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/ChangeLog-8.php#

Affected Product	**NETGEAR**
Severity	**High**
Affected Vulnerability	Post-Authentication Command Injection Vulnerability
Description	NETGEAR has released a security update addressing a Post-Authentication Command Injection Vulnerability that exists in their products. This vulnerability requires an attacker to have your WiFi password or an Ethernet connection to a device on your network as well as the admin login and password to your network to be exploited. NETGEAR advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NETGEAR Router R8000 firmware versions before 1.0.4.88
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000066209/Security-Advisory-for-Post-Authentication-Command-Injection-on-the-R8000-PSV-2024-0022

Affected Product	**PHP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-5585, CVE-2024-5458)
Description	PHP has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-5585** - The vulnerability exists due to insufficient fix for CVE-2024-1874. A remote attacker can pass specially crafted input to the application and execute arbitrary OS commands on the target system. **CVE-2024-5458** - The vulnerability exists due to insufficient validation of user-supplied input when parsing URL. A remote attacker can bypass the filter_var FILTER_VALIDATE_URL checks. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20 and 8.3.* before 8.3.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/ChangeLog-8.php#

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-13631, CVE-2019-15505, CVE-2020-25656, CVE-2021-3753, CVE-2021-4204, CVE-2022-0500, CVE-2022-23222, CVE-2022-3565, CVE-2022-45934, CVE-2023-1513, CVE-2023-24023, CVE-2023-25775, CVE-2023-28464, CVE-2023-31083, CVE-2023-3567, CVE-2023-37453, CVE-2023-38409, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-39198, CVE-2023-4133, CVE-2023-4244, CVE-2023-42754, CVE-2023-42755, CVE-2023-45863, CVE-2023-51779, CVE-2023-51780, CVE-2023-52340, CVE-2023-52434, CVE-2023-52448, CVE-2023-6121, CVE-2023-6176, CVE-2023-6622, CVE-2023-6915, CVE-2023-6932, CVE-2024-0841, CVE-2024-26602, CVE-2024-26609, CVE-2023-52489, CVE-2023-52574, CVE-2023-52580, CVE-2023-52581, CVE-2023-52620, CVE-2024-25742, CVE-2024-25743, CVE-2024-26671, CVE-2024-22259, CVE-2023-4408, CVE-2023-50387, CVE-2023-50868, CVE-2023-40546, CVE-2023-40547, CVE-2023-40548, CVE-2023-40549, CVE-2023-40550, CVE-2023-40551, CVE-2024-22243, CVE-2023-3758, CVE-2024-22262)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of service, Phishing attacks, Arbitrary code execution, Sensitive information disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP8 IF02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7156774 • https://www.ibm.com/support/pages/node/7156667

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of service, User after free conditions, Null pointer deference, Integer overflow. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6816-1

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.