Advisory Alert

Alert Number: AAA20251211 **Date:** December 11, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Barracuda	**Critical**	Multiple Vulnerabilities
Barracuda	**High**	Path Traversal Vulnerability
IBM	**High**, **Medium**	Multiple Out-of-Bounds Read Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Security Update
NETGEAR	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Barracuda**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-34392, CVE-2025-34393, CVE-2025-34394)
Description	Barracuda has released a security update addressing multiple vulnerabilities that impacts the Barracuda RMM Service Center. **CVE-2025-34392:** Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, does not verify the URL defined in an attacker-controlled WSDL that is later loaded by the application. This can lead to arbitrary file write and remote code execution via webshell upload. **CVE-2025-34393:** Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, does not correctly verify the name of an attacker-controlled WSDL service, leading to insecure reflection. This can result in remote code execution through either invocation of arbitrary methods or deserialization of untrusted types. **CVE-2025-34394:** Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, exposes a .NET Remoting service that is insufficiently protected against deserialization of arbitrary types. This can lead to remote code execution. Barracuda advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Barracuda RMM Service Center versions prior to 2025.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://trust.barracuda.com/security/information/rce-vulnerabilities-barracuda-rmm-service-center-hotfix-availabile

Affected Product	**Barracuda**
Severity	**High**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2025-34395)
Description	Barracuda has released a security update addressing an improper path validation vulnerability that impacts the Barracuda RMM Service Center. **CVE-2025-34395:** Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, exposes a .NET Remoting service in which an unauthenticated attacker can invoke a method vulnerable to path traversal to read arbitrary files. This vulnerability can be escalated to remote code execution by retrieving the .NET machine keys. Barracuda advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Barracuda RMM Service Center versions prior to 2025.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://trust.barracuda.com/security/information/rce-vulnerabilities-barracuda-rmm-service-center-hotfix-availabile

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Out-of-Bounds Read Vulnerabilities (CVE-2025-9230, CVE-2025-9232)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-9230:** An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. **CVE-2025-9232:** An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no_proxy' environment variable is set and the host portion of the authority component of the HTTP URL is an IPv6 address. An out-of-bounds read can trigger a crash which leads to Denial of Service for an application. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AIX versions 7.2 and 7.3 VIOS versions 3.1 and 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7254361

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40018, CVE-2025-39993, CVE-2025-39964, CVE-2025-38666, CVE-2025-37958, CVE-2025-21855, CVE-2024-53218, CVE-2024-53090, CVE-2024-50196, CVE-2024-50095, CVE-2024-50067, CVE-2024-49935, CVE-2024-47691, CVE-2022-49390, CVE-2022-49026, CVE-2025-39946, CVE-2025-40232)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 25.10, 25.04, 24.04, 20.04 and 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7922-1 • https://ubuntu.com/security/notices/USN-7921-1 • https://ubuntu.com/security/notices/USN-7920-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-38737)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-38737:** cifs: Fix oops due to uninitialised variable Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:23009

Affected Product	**NETGEAR**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12941, CVE-2025-12946, CVE-2025-12945)
Description	NetGear has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-12941:** Denial of Service Vulnerability in NETGEAR C6220 and C6230 (DOCSIS 3.0 Two-in-one Cable Modem + Wi-Fi Router) allows authenticated local WiFi users reboot the router. **CVE-2025-12946:** A vulnerability in the speedtest feature of affected NETGEAR Nighthawk routers, caused by improper input validation, can allow attackers on the router's WAN side, using attacker-in-the-middle techniques (MiTM) to manipulate DNS responses and execute commands when speedtests are run. **CVE-2025-12945:** A vulnerability in NETGEAR Nighthawk R7000P routers lets an authenticated admin execute OS command injections due to improper input validation. NetGear advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	C6220 and C6230 NETGEAR Nighthawk Routers: • RS700: through 1.0.7.82 • RAX54Sv2 : before V1.1.6.36 • RAX41v2: before V1.1.6.36 • RAX50: before V1.2.14.114 • RAXE500: before V1.2.14.114 • RAX41: before V1.0.17.142 • RAX43: before V1.0.17.142 • RAX35v2: before V1.0.17.142 • RAXE450: before V1.2.14.114 • RAX43v2: before V1.1.6.36 • RAX42: before V1.0.17.142 • RAX45: before V1.0.17.142 • RAX50v2: before V1.1.6.36 • MR90: before V1.0.2.46 • MS90: before V1.0.2.46 • RAX42v2: before V1.1.6.36 • RAX49S: before V1.1.6.36 • R7000P: through 1.3.3.154
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000070416/December-2025-NETGEAR-Security-Advisory

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.