Advisory Alert

Alert Number: **AAA20230612** **Date:** **June 12, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Netgear	**High**	Stack overflow Vulnerability

Description

Affected Product	**Netgear**
Severity	**High**
Affected Vulnerability	Stack overflow Vulnerability (CVE-2023-34285)
Description	Netgear has released a security update addressing a Pre-Authentication Stack overflow vulnerability that exist in their RAX30 Router. **CVE-2023-34285** - If the attacker is able to obtain the WiFi password or an Ethernet connection to a device on the network as well as the admin login and password on the network, he or she is capable of performing the Pre-Authentication Stack Overflow. Netgear recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	RAX30 firmware versions prior 1.0.11.96_2_HOTFIX
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000065701/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-the-RAX30-PSV-2023-0038

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.