The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
11/18/2021

SUBJECT:
A Vulnerability in Multiple NETGEAR Products Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in multiple NETGEAR products, which could allow for arbitrary code execution. Successful exploitation of this vulnerability could allow for arbitrary code execution in the context of the root user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
GRIMM researchers are reported to have an exploit capable of compromising fully patched devices that are running the default configuration.

SYSTEMS AFFECTED:

- NetGear AirCards prior to firmware version 1.0.0.62
- NetGear Cable Modems prior to firmware version 2.1.3.5
- NetGear DSL Modem Routers D7000v2 and D6220 prior to firmware version 1.0.0.76
- NetGear DSL Modem Routers D6400 prior to firmware version 1.0.0.108
- NetGear DSL Modem Routers D6400 prior to firmware version 1.0.0.126
- NetGear Extenders EX3700 and EX3800 prior to firmware version 1.0.0.94
- NetGear Extenders EX6120 and EX6130 prior to firmware version 1.0.0.66
- NetGear Routers See NetGear release under references for full list of patched firmware versions.

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in multiple NETGEAR products, which could allow for arbitrary code execution. The specific flaw exists within the UPnP service, which listens on TCP port 5000 by default. When parsing the uuid request header, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.

Successful exploitation of this vulnerability could allow for arbitrary code execution in the context of the root user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by NETGEAR to vulnerable systems immediately after appropriate testing.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:

NETGEAR:

https://kb.netgear.com/000064361/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Multiple-Products-PSV-2021-0168

GITHUB:

https://github.com/grimm-co/NotQuite0DayFriday/tree/trunk/2021.11.16-netgear-upnp

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34991

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.