TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2017-095

DATE ISSUED:
10/05/2017

SUBJECT:
Critical Patches Issued for Netgear Products, October 4, 2017

OVERVIEW:
Multiple vulnerabilities have been discovered in Netgear products, the most severe of which could allow for arbitrary code execution. Netgear is a manufacturer of networked devices such as Network Attached Storage (NAS), routers, switches, cable and DSL modems, and video cameras. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code and gain full control of the affected system. Failed exploit attempts could result in a denial of service condition.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- D500/D1500 running firmware versions prior 1.0.0.25
- D6100 running firmware versions prior to 1.0.0.50_0.0.50
- D6220 running firmware versions prior to 1.0.0.28
- D6400 running firmware versions prior to 1.0.0.60
- D7000 running firmware versions prior to 1.0.1.50
- D7800 running firmware versions prior to 1.0.1.22
- D8500 running firmware versions prior to 1.0.3.28
- EX6200v2 running firmware versions prior to 1.0.1.50
- JNR1010v2 running firmware versions prior to 1.1.0.40
- JWNR2010v5 running firmware versions prior to 1.1.0.40
- PR2000 running firmware versions prior to 1.0.0.17
- R6050/JR6150 running firmware versions prior to 1.0.1.7
- R6100 running firmware versions prior to 1.0.1.14
- R6200v2 running firmware versions prior to 1.0.3.14
- R6220 running firmware versions prior to 1.1.0.50
- R6250 running firmware versions prior to 1.0.4.8
- R6300v2 running firmware versions prior to 1.0.4.8
- R6400 running firmware versions prior to 1.0.1.22
- R6400v2 running firmware versions prior to 1.0.2.32
- R6700 running firmware versions prior to 1.0.1.26
- R6700v2 running firmware versions prior 1.1.0.38
- R6800 running firmware versions prior 1.1.0.38
- R6900 running firmware versions prior to 1.0.1.28
- R7000 running firmware versions prior to 1.0.7.10
- R7000P/R6900P running firmware versions prior to 1.0.0.56
- R7100LG running firmware versions prior to 1.0.0.30
- R7300 running firmware versions prior to 1.0.0.52
- R7500 running firmware versions prior to 1.0.0.110

- R7500v2 running firmware versions prior to 1.0.3.16
- R7800 running firmware versions prior to 1.0.2.32
- R7900 running firmware versions prior to 1.0.1.14
- R8000 running firmware versions prior to 1.0.3.22
- R8300 running firmware versions prior to 1.0.2.94
- R8500 running firmware versions prior to 1.0.2.74
- WNDR3700v5 running firmware versions prior to 1.1.0.48
- WNR1000v4 running firmware versions prior to 1.1.0.40
- WNR2020 running firmware versions prior to 1.1.0.40
- WNR2050 running firmware versions prior to 1.1.0.40
- WNR614 running firmware versions prior to 1.1.0.40
- WNR618 running firmware versions prior to 1.1.0.40

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

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

Home users: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Netgear products, the most severe of which could allow for arbitrary code execution.

A full list of all vulnerabilities can be found at the link below:
https://www.netgear.com/about/security/

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code and gain full control of the affected system. Failed exploit attempts could result in a denial of service condition.

RECOMMENDATIONS:
We recommend the following actions be taken:
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Apply patch provided by Netgear immediately after appropriate testing.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:
Netgear:
https://www.netgear.com/about/security

Threatpost:
https://threatpost.com/netgear-fixes-50-vulnerabilities-in-routers-switches-nas-devices/128230

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/