tenable

Netgear Nighthawk R6700 Multiple Vulnerabilities

High

← View More Research Advisories

Synopsis

The following security-related issues have been found in the latest available firmware for the Nighthawk R6700v3 AC1750 consumer routing device (1.0.4.120 at the time of this writing).

Post Authentication Command Injection via SOAP Interface - CVE-2021-20173

We have identified 3 instances of unsanitized input being sent to system() calls in the upnpd binary, which runs by default.

The following request can be used to force an update check from the SOAP interface (note: this requires authenticating prior):

```
POST /soap/server_sa/ HTTP/1.0
SOAPAction: urn:NETGEAR-ROUTER:service:DeviceConfig:1#CheckNewFirmware
content-type: text/xml;charset=utf-8
HOST: routerlogin.net
User-Agent: SOAP Toolkit 3.0
Connection: close
Cache-Control: no-cache
Pragma: no-cache
Cookie: sess_id=018b49310551ca2de378a56e5f03294bc4c58e2b2dd8671d211abfbddaeb932dd8b60666d6c406356e71620c004fa226094ab2888d422f7133bf377490278819; SameSite=Strict
Content-Length: 525

<?xml version="1.0" encoding="UTF-8" standalone="no"?><SOAP-ENV:Envelope xmlns:SOAPSDK1="http://www.w3.org/2001/XMLSchema" xmlns:SOAPSDK2="http://www.w3.org/2001/XMLSchema-instance"
xmlns:SOAPSDK3="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header><SessionID>E6A88AE69687E58D9A00</SessionID></SOAP-ENV:Header><SOAP-ENV:Body><M1:CheckNewFirmware
xmlns:M1="urn:NETGEAR-ROUTER:service:DeviceConfig:1"></M1:CheckNewFirmware></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

The following system() commands pull values from the device's configuration and run them directly on the device when the above request is sent:

```
Instance 1:
    snprintf(acStack640,0x200,
             "rm -f %s %s %s;wget -b --tries=2 --timeout=5 -o %s --ca-certificate /opt/xagent/certs/%s -O %s \'https://%s/%s/%s/%s\' &"
             ,"/tmp/stringtable.dat","/tmp/wget-log-upnp-strdat","/var/run/wget.pid",
             "/tmp/wget-log-upnp-strdat",&local_40,"/tmp/stringtable.dat",uVar1,acStack128,uVar2,
             uVar3);
    FUN_0000c310(3,"[upnp_sa] wget_SendGetStrDatCmd:%s\n",acStack640);
    system(acStack640);

Instance 2:
  snprintf(acStack712,0x200,
           "rm -f %s %s %s;wget -b --tries=2 --timeout=5 -o %s --ca-certificate /opt/xagent/certs/%s -O %s \'https://%s/%s/%s/%s\' &"
           ,"/tmp/firmwareCfg","/tmp/wget-log-upnp-finfo","/var/run/wget.pid",
           "/tmp/wget-log-upnp-finfo",&local_48,"/tmp/firmwareCfg",uVar1,acStack200,uVar2,uVar3);
  FUN_0000c310(3,"[upnp_sa] wget_SendGetCfgCmd:%s\n",acStack712);
  system(acStack712);

Instance 3:
    snprintf(acStack632,0x200,
             "rm -f %s %s %s;wget -b --tries=2 --timeout=5 -o %s --ca-certificate /opt/xagent/certs/%s -O %s https://%s/%s/%s/%s &"
             ,"/tmp/image.chk","/tmp/wget-log-upnp-img","/var/run/wget.pid","/tmp/wget-log-upnp-img"
             ,&local_38,"/tmp/image.chk",uVar1,acStack120,uVar2,&DAT_000c10d0);
```

Each of the above commands are executed when updates are checked for via the upnpd binary and can be injected with the corresponding configuration values. For example, by modifying the "ver_check_stringtable_dat" variable to use something like "stringtable.dat'; echo hi; #" will cause instance 1 to run "echo hi" when checking for updates. We have assigned a CVSS vector of CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H to these issues.

Default HTTP Communication (Web Interface) - CVE-2021-20174

By default, all communication to/from the device's web interface is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext. We recommend using HTTPS as the default.

CVSS score of CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N.

Default HTTP Communication (SOAP Interface) - CVE-2021-20175

By default, all communication to/from the device's SOAP Interface (port 5000) is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext. We recommend using HTTPS as the default.

CVSS score of CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N.

Insufficient UART Protection Mechanisms - CVE-2021-23147

A malicious actor with physical access to the device is able to connect to the UART port via a serial connection and execute commands as the root user without authentication. We recommend disabling this UART console for production runs, or at least enforcing the same password mechanisms used for other functionality in the device (such as the web UI).

CVSS score of CVSS:3.0/AV: P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Configuration Manipulation via Hardcoded Encryption Routines - CVE-2021-45732

It does not appear that normal users are intended to be able to manipulate configuration backups due to the fact that they are encrypted/obfuscated. By extracting the configuration using readily available public tools, a user can reconfigure settings not intended to be manipulated, repackage the configuration, and restore a backup causing these settings to be changed.

CVSS score of CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H.

Plaintext Password Storage - CVE-2021-45077

All usernames and passwords for the device's associated services are stored in plaintext on the device. For example, the admin password is stored in plaintext in the primary configuration file on the device.

CVSS score of CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

Known Vulnerable minidlna.exe Service

The version of minidlna.exe running on the device contains publicly known vulnerabilities. We recommend upgrading to a more recent version.

Solution

Tenable has not been informed of any available patches for these issues at the time of this writing.

Disclosure Timeline

September 30, 2021 - Tenable discloses to vendor.
October 4, 2021 - Vendor provides formal acknowledgment.
October 7, 2021 - Vendor requests clarification. Tenable needs more information from vendor. Vendor supplies information.
October 8, 2021 - Tenable provides testing suggestions.
October 26, 2021 - Tenable requests status update.
November 12, 2021 - Vendor provides status update.

Risk Information

CVE ID: CVE-2021-20173
CVE-2021-20174
CVE-2021-20175
CVE-2021-23147
CVE-2021-45732
CVE-2021-45077
Tenable Advisory ID: TRA-2021-57
Credit: Jimi Sebree

CVSSv3 Base / Temporal Score: 7.1 / 6.7
CVSSv3 Vector: AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Affected Products: Netgear Nighthawk R6700 1.0.4.120
Risk Factor: High

Advisory Timeline

December 30, 2021 - Initial release.

State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media