

Support (<http://www.netgear.com/support/>) / Home & Mobile WiFi (<https://www.netgear.com/support/home/>) / Knowledge Base (<https://www.netgear.com/support/home/kb/>) / Security (<https://www.netgear.com/support/home/kb/category?name=Security>) / June 2026 NETGEAR Security Advisory

# June 2026 NETGEAR Security Advisory

NETGEAR's Product Security Team has assessed the following product vulnerabilities and provided guidance to address these vulnerabilities in the table below.

Because firmware updates contain security fixes, bug fixes, and new features for your products, we strongly advise you to enable automatic firmware updates on supported devices. For older products, we advise you to download and install new firmware updates as soon as possible or follow the guidance provided for devices that require other remediation steps.

### Affected Products



**MR70** (<https://www.netgear.com/support/product/mr70/>), **MS70** (<https://www.netgear.com/support/product/ms70/>)



**RAXE500** (<https://www.netgear.com/support/product/raxe500/>), **XR1000** (<https://www.netgear.com/support/product/xr1000/>)

### CVE-2026-9213 Insufficient input validation in certain NETGEAR routers

A vulnerability in the affected NETGEAR gaming routers allows attackers with the ability to intercept and tamper traffic between the router and the Internet, to execute code on the device.

Severity: **MEDIUM** (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AN%2FAC%3AH%2FAT%3AP%2FPR%3AN%2FUI%3AN%2FVC%3AH%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU>)

Acknowledgments: fluorescent

### Recommendation

If automatic updates are enabled, your device may already have this security update applied. If not, please check the firmware version and install the latest update. Fixed in:

| Product | Fixed Version                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------|
| MR70    | V1.0.4.48 ( <a href="https://www.netgear.com/support/product/mr70/">https://www.netgear.com/support/product/mr70/</a> )         |
| MS70    | V1.0.4.48 ( <a href="https://www.netgear.com/support/product/ms70/">https://www.netgear.com/support/product/ms70/</a> )         |
| RAXE500 | V1.2.14.114 ( <a href="https://www.netgear.com/support/product/raxe500/">https://www.netgear.com/support/product/raxe500/</a> ) |
| XR1000  | V1.0.2.86 ( <a href="https://www.netgear.com/support/product/xr1000/">https://www.netgear.com/support/product/xr1000/</a> )     |

Affected Products



**LBR1020** **LBR20** (<https://www.netgear.com/support/product/lbr20/>)



**R6700AX** (<https://www.netgear.com/support/product/R6700AX/>) **R7800** (<https://www.netgear.com/support/product/r7800/>)



**R9000** (<https://www.netgear.com/support/product/r9000/>) **RAX10** (<https://www.netgear.com/support/product/rax10/>)



**RAX10v2** (<https://www.netgear.com/support/product/RAX10v2/>) **RAX120** (<https://www.netgear.com/support/product/rax120/>)



**RAX120v1** **RAX120v2** (<https://www.netgear.com/support/product/RAX120v2/>)



**RAX36S** (<https://www.netgear.com/support/product/RAX36S/>) **RAX70** (<https://www.netgear.com/support/product/rax70/>)



**RAX78** (<https://www.netgear.com/support/product/RAX78/>) **RBR10**



**RBR20** (<https://www.netgear.com/support/product/rbr20/>) **RBR350** (<https://www.netgear.com/support/product/rbr350/>)



**RBR40** **RBR50** (<https://www.netgear.com/support/product/rbr50/>)



**RBS10** (<https://www.netgear.com/support/product/rbs10/>) **RBS20** (<https://www.netgear.com/support/product/rbs20/>)



**RBS350** (<https://www.netgear.com/support/product/rbs350/>) **RBS40** (<https://www.netgear.com/support/product/rbs40/>)



**RBS50** (<https://www.netgear.com/support/product/rbs50/>) **XR450** (<https://www.netgear.com/support/product/XR450/>)



**XR500** (<https://www.netgear.com/support/product/xr500/>)

**CVE-2026-9212 Insufficient authentication and input validation in certain NETGEAR products**

Insufficient authentication and input validation in the listed NETGEAR models allow users connected to the local network to execute commands impacting product's confidentiality or change certain configurations.

Severity: MEDIUM (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AL%2FUI%3AN%2FVC%3AH%2FVI%3AL%2FVA%3AN%2FSC%3AH%2FSI%3AN%2FSA%3AN%2FE%3AU>)

Acknowledgments: ZeroZenx Labs

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

|          |                                                                                                                               |
|----------|-------------------------------------------------------------------------------------------------------------------------------|
| Product  | Fixed Version                                                                                                                 |
| LBR1020* | V2.6.4.60 ( <a href="https://www.netgear.com/support/product/lbr1020/">https://www.netgear.com/support/product/lbr1020/</a> ) |

| Product   | Fixed Version                                                                                                                  |
|-----------|--------------------------------------------------------------------------------------------------------------------------------|
| LBR20     | <a href="https://www.netgear.com/support/product/lbr20/">V2.7.6.8 (https://www.netgear.com/support/product/lbr20/)</a>         |
| R6700AX*  | EOS                                                                                                                            |
| R7800*    | <a href="https://www.netgear.com/support/product/r7800/">V1.0.4.96 (https://www.netgear.com/support/product/r7800/)</a>        |
| R9000*    | <a href="https://www.netgear.com/support/product/r9000/">V1.0.6.46 (https://www.netgear.com/support/product/r9000/)</a>        |
| RAX10     | <a href="https://www.netgear.com/support/product/rax10/">V1.0.5.50 (https://www.netgear.com/support/product/rax10/)</a>        |
| RAX10v2   | V1.0.5.50                                                                                                                      |
| RAX120    | <a href="https://www.netgear.com/support/product/rax120/">V1.2.10.56 (https://www.netgear.com/support/product/rax120/)</a>     |
| RAX120v1* | V1.2.10.56                                                                                                                     |
| RAX120v2  | <a href="https://www.netgear.com/support/product/rax120v2/">V1.2.10.56 (https://www.netgear.com/support/product/rax120v2/)</a> |
| RAX36S    | <a href="https://www.netgear.com/support/product/rax36s/">V1.0.5.50 (https://www.netgear.com/support/product/rax36s/)</a>      |
| RAX70     | <a href="https://www.netgear.com/support/product/rax70/">V1.0.19.172 (https://www.netgear.com/support/product/rax70/)</a>      |
| RAX78     | <a href="https://www.netgear.com/support/product/rax78/">V1.0.19.172 (https://www.netgear.com/support/product/rax78/)</a>      |
| RBR10*    | EOS                                                                                                                            |
| RBR20*    | EOS                                                                                                                            |
| RBR350    | <a href="https://www.netgear.com/support/product/rbr350/">V4.4.2.1 (https://www.netgear.com/support/product/rbr350/)</a>       |
| RBR40*    | EOS                                                                                                                            |
| RBR50*    | EOS                                                                                                                            |
| RBS10*    | EOS                                                                                                                            |
| RBS20*    | EOS                                                                                                                            |
| RBS350    | <a href="https://www.netgear.com/support/product/rbs350/">V4.4.2.1 (https://www.netgear.com/support/product/rbs350/)</a>       |
| RBS40*    | EOS                                                                                                                            |
| RBS50*    | EOS                                                                                                                            |
| XR450*    | <a href="https://www.netgear.com/support/product/xr450/">V2.3.3.136 (https://www.netgear.com/support/product/xr450/)</a>       |
| XR500*    | <a href="https://www.netgear.com/support/product/xr500/">v2.3.3.136 (https://www.netgear.com/support/product/xr500/)</a>       |

\* Model has reached its End-of-Support (EOS) phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

Affected Products



**[CAX30 \(https://www.netgear.com/support/product/cax30/\)](https://www.netgear.com/support/product/cax30/)** **[RAX30 \(https://www.netgear.com/support/product/rax30/\)](https://www.netgear.com/support/product/rax30/)**



**[RAX5 \(https://www.netgear.com/support/product/rax5/\)](https://www.netgear.com/support/product/rax5/)** **[RAXE300 \(https://www.netgear.com/support/product/raxe300/\)](https://www.netgear.com/support/product/raxe300/)**

CVE-2026-9211 Certain NETGEAR routers allow unauthenticated users to gain control of the router

An unauthenticated user on the local network can gain control of the router and make unauthorized changes to its operation.

Severity: MEDIUM(<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AP%2FPR%3AN%2FU%3AN%2FVC%3AH%2FVI%3AH%2FVA%3AH%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FV%3AD%2FRE%3AL%2FU%3AAMber>)

Acknowledgments: kaoken

Recommendation

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product | Fixed Version                                                                                                                  |
|---------|--------------------------------------------------------------------------------------------------------------------------------|
| CAX30   | V2.2.1.4                                                                                                                       |
| RAX30   | V1.0.10.94                                                                                                                     |
| RAX5    | V1.0.5.34 ( <a href="https://www.netgear.com/support/product/rax5/">https://www.netgear.com/support/product/rax5/</a> )        |
| RAXE300 | V1.0.10.72 ( <a href="https://www.netgear.com/support/product/raxe300/">https://www.netgear.com/support/product/raxe300/</a> ) |

Affected Products



**RBR860** (<https://www.netgear.com/support/product/rbr860/>) **RBRE950** (<https://www.netgear.com/support/product/rbre950/>)



**RBRE960** (<https://www.netgear.com/support/product/rbre960/>) **RBRE970** (<https://www.netgear.com/support/product/RBE970/>)



**RBSE971** (<https://www.netgear.com/support/product/RBE971/>) **RBS860** (<https://www.netgear.com/support/product/rbs860/>)



**RBSE950** (<https://www.netgear.com/support/product/rbse950/>)



**RBSE960** (<https://www.netgear.com/support/product/rbse960/>)

CVE-2026-3088 Unauthenticated users can disrupt router operation

Unauthenticated users on the local network can cause the router to become unavailable by sending specially crafted requests.

Acknowledgments: fxc233

Issue fixed in:

|         |                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------|
| Product | Fixed Version                                                                                                               |
| RBR860  | <a href="https://www.netgear.com/support/product/rbr860/">V7.2.7.15 (https://www.netgear.com/support/product/rbr860/)</a>   |
| RBRE950 | <a href="https://www.netgear.com/support/product/rbre950/">v7.2.7.15 (https://www.netgear.com/support/product/rbre950/)</a> |
| RBRE960 | <a href="https://www.netgear.com/support/product/rbre960/">V7.2.7.15 (https://www.netgear.com/support/product/rbre960/)</a> |
| RBE970  | V9.10.1.4                                                                                                                   |
| RBE971  | V9.10.1.4                                                                                                                   |
| RBS860  | <a href="https://www.netgear.com/support/product/rhs860/">V7.2.7.15 (https://www.netgear.com/support/product/rhs860/)</a>   |
| RBSE950 | <a href="https://www.netgear.com/support/product/rbse950/">v7.2.7.15 (https://www.netgear.com/support/product/rbse950/)</a> |
| RBSE960 | <a href="https://www.netgear.com/support/product/rbse960/">V7.2.7.15 (https://www.netgear.com/support/product/rbse960/)</a> |

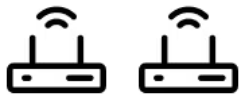
A white wireless router with two antennas. The front panel features a power jack, a power button, and a small display screen. The brand name 'NETGEAR' is visible on the front. The back panel has several ports, including a power port and a USB port.



night hawk



6/26

**R6400v2****R6700v3****R6900P** (<https://www.netgear.com/support/product/r6900p/>)**R7000** (<https://www.netgear.com/support/product/r7000/>) **R7000P** (<https://www.netgear.com/support/product/r7000p/>)**R7960P** (<https://www.netgear.com/support/product/r7960p/>) **R8000P** (<https://www.netgear.com/support/product/r8000p/>)**R8500** (<https://www.netgear.com/support/product/r8500/>) **RAX20** (<https://www.netgear.com/support/product/rax20/>)**RAX35v2** (<https://www.netgear.com/support/product/rax35v2/>)**RAX40v2** (<https://www.netgear.com/support/product/RAX40v2/>) **RAX41** (<https://www.netgear.com/support/product/rax41/>)**RAX42** (<https://www.netgear.com/support/product/rax42/>) **RAX43** (<https://www.netgear.com/support/product/rax43/>)**RAX45** (<https://www.netgear.com/support/product/rax45/>) **RAX48** (<https://www.netgear.com/support/product/RAX48/>)**RAX50** (<https://www.netgear.com/support/product/rax50/>) **RAX50S** (<https://www.netgear.com/support/product/RAX50S/>)



**RAXE450** (<https://www.netgear.com/support/product/raxe450/>)



**RAXE500** (<https://www.netgear.com/support/product/raxe500/>) **XR1000** (<https://www.netgear.com/support/product/xr1000/>)

**CVE-2026-9210 Certain NETGEAR routers allow authenticated administrators to gain unintended control of the router**

Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.

Severity: MEDIUM (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AN%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FV%3AD%2FRE%3AL%2FU%3A%2FAmber>)

Acknowledgments: pjqwudi

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product  | Fixed Version                                                                                                                |
|----------|------------------------------------------------------------------------------------------------------------------------------|
| EX3700   | V1.0.0.100 ( <a href="https://www.netgear.com/support/product/ex3700/">https://www.netgear.com/support/product/ex3700/</a> ) |
| EX3800*  | V1.0.0.100 ( <a href="https://www.netgear.com/support/product/ex3800/">https://www.netgear.com/support/product/ex3800/</a> ) |
| EX6120   | V1.0.0.72 ( <a href="https://www.netgear.com/support/product/ex6120/">https://www.netgear.com/support/product/ex6120/</a> )  |
| EX6130   | V1.0.0.54 ( <a href="https://www.netgear.com/support/product/ex6130/">https://www.netgear.com/support/product/ex6130/</a> )  |
| MR60     | V1.1.7.132                                                                                                                   |
| MR70     | V1.0.3.28                                                                                                                    |
| MR80     | V1.1.7.14                                                                                                                    |
| MS60     | V1.1.7.132                                                                                                                   |
| MS70     | V1.0.3.28                                                                                                                    |
| MS80     | V1.1.7.14                                                                                                                    |
| R6400v2* | V1.0.4.128                                                                                                                   |
| R6700v3* | V1.0.4.128                                                                                                                   |
| R6900P*  | V1.3.3.152                                                                                                                   |
| R7000*   | V1.0.11.216                                                                                                                  |
| R7000P*  | V1.3.3.152                                                                                                                   |
| R7960P*  | V1.4.4.92                                                                                                                    |
| R8000P*  | V1.4.4.92                                                                                                                    |
| R8500*   | EoS                                                                                                                          |
| RAX20*   | V1.0.18.144 ( <a href="https://www.netgear.com/support/product/rax20/">https://www.netgear.com/support/product/rax20/</a> )  |
| RAX35v2  | V1.0.12.118                                                                                                                  |
| RAX40v2  | V1.0.12.118                                                                                                                  |

| Product | Fixed Version |
|---------|---------------|
| RAX41*  | V1.0.12.118   |
| RAX42*  | V1.0.12.118   |
| RAX43*  | V1.0.12.120   |
| RAX45*  | V1.0.12.118   |
| RAX48   | V1.0.12.118   |
| RAX50   | V1.0.12.120   |
| RAX50S  | V1.0.12.120   |
| RAXE450 | V1.0.10.86    |
| RAXE500 | V1.0.10.86    |
| XR1000  | V1.0.0.68     |

\* Model has reached its End-of-Support phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

Affected Products



**Orbi 370** ([https://www.netgear.com/support/product/Orbi 370](https://www.netgear.com/support/product/Orbi%20370))

**CVE-2026-0409 Netgear Orbi 370 Series Remote Code Execution vulnerability**

A NETGEAR security issue that could allow an attacker with ability to intercept and tamper with traffic between the router and the Internet to run commands on your device when the device administrator performs certain specific management actions. This issue affects NETGEAR Orbi 370 series devices before V12.1.2.7.

Severity: MEDIUM (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AN%2FAC%3AH%2FAT%3AP%2FPR%3AN%2FUI%3AA%2FVC%3AH%2FVI%3AH%2FVA%3AH%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU>)

Acknowledgments: ChinaNuke

Recommendation

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product                                                  | Fixed Version                                                                                                               |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| NETGEAR Orbi 370 series (RBE370, RBE371, RBE372, RBE374) | V12.1.2.7 ( <a href="https://www.netgear.com/support/product/rbe372/">https://www.netgear.com/support/product/rbe372/</a> ) |

Affected Products



**RAX120v1 RAX120v2** (<https://www.netgear.com/support/product/RAX120v2>)



**RAX35** (<https://www.netgear.com/support/product/rax35/>) **RAX38**



**RAX40** (<https://www.netgear.com/support/product/rax40/>)

**CVE-2026-0420 Missing TLS certificate validation in ReadyCloud client app**

An improper implementation of TLS certificate validation vulnerability found in ReadyCloud client app which can allow an attacker to perform attacker-in-the-middle (MiTM) style attacks impacting product's confidentiality. This vulnerability affects the listed NETGEAR models.

Severity: **MEDIUM** (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AN%2FAC%3AH%2FAT%3AP%2FPR%3AN%2FUI%3AN%2FVC%3AH%2FVI%3AN%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU>)

Acknowledgments: talsonor

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product   | Fixed Version                                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------------------------------------|
| RAX120v1* | V1.2.9.52                                                                                                                     |
| RAX120v2  | <a href="https://www.netgear.com/support/product/rax120v2/">V1.2.9.52 (https://www.netgear.com/support/product/rax120v2/)</a> |
| RAX35*    | <a href="https://www.netgear.com/support/product/rax35/">V1.0.6.106 (https://www.netgear.com/support/product/rax35/)</a>      |
| RAX38*    | <a href="https://www.netgear.com/support/product/rax38/">V1.0.6.106 (https://www.netgear.com/support/product/rax38/)</a>      |
| RAX40*    | <a href="https://www.netgear.com/support/product/rax40/">V1.0.6.106 (https://www.netgear.com/support/product/rax40/)</a>      |

\* Model has reached its End-of-Support phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

**Affected Products**



**JR6150** (<https://www.netgear.com/support/product/jr6150/>)

**CVE-2026-0419 Insufficient input validation vulnerability in NETGEAR JR6150**

Insufficient input validation in NETGEAR JR6150 (AC750 WiFi Router 802.11ac Dual Band Gigabit released in 2014) allows users connected to the local WiFi Networks to execute operating system commands. NETGEAR JR6150 has reached End-of-Support phase as of 2018 , and no further security updates are planned. NETGEAR strongly recommends replacing these devices with newer NETGEAR models to ensure continued security support and updates.

This vulnerability has been identified through firmware emulation in a controlled research environment and has not been verified on production hardware.

CVSS%3A4.0%2FAV%3AL%2FAC%3AL%2FAT%3AP%2FPR%3AL%2FUI%3AN%2FVC%3AH%2FVI%3AH%2FVA%3AH%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FV%3AD%2FRE%3AL%2FU%3AAmber)

## Recommendation

## Affected Products



A black wireless router with two antennas, positioned horizontally. The front panel features a series of small, illuminated status lights.



A black wireless router with two antennas, positioned at the bottom of the page.

11/26



**RAX38v2** (<https://www.netgear.com/support/product/RAX38v2/>)



**RAX40v2** (<https://www.netgear.com/support/product/RAX40v2/>) **RAX42** (<https://www.netgear.com/support/product/rax42/>)



**RAX43** (<https://www.netgear.com/support/product/rax43/>) **RAX45** (<https://www.netgear.com/support/product/rax45/>)



**RAX48** (<https://www.netgear.com/support/product/RAX48/>) **RAX50** (<https://www.netgear.com/support/product/rax50/>)



**RAX50S** (<https://www.netgear.com/support/product/RAX50S/>) **RAX75**



**RAX80** (<https://www.netgear.com/support/product/rax80/>) **RAXE450** (<https://www.netgear.com/support/product/raxe450/>)



**RAXE500** (<https://www.netgear.com/support/product/raxe500/>) **RBR750** (<https://www.netgear.com/support/product/rbr750/>)



**RBR840** (<https://www.netgear.com/support/product/rbr840/>) **RBR850** (<https://www.netgear.com/support/product/rbr850/>)



**RBRE960** (<https://www.netgear.com/support/product/rbre960/>) **RBS750** (<https://www.netgear.com/support/product/rbs750/>)



**RBS840** (<https://www.netgear.com/support/product/rbs840/>) **RBS850** (<https://www.netgear.com/support/product/rbs850/>)



**RBSE960** (<https://www.netgear.com/support/product/rbse960/>) **RS700** (<https://www.netgear.com/support/product/rs700/>)



**XR1000** (<https://www.netgear.com/support/product/xr1000/>)

**CVE-2026-0418 Certain NETGEAR devices allow administrators to tamper with system**

Insufficient configuration management in the listed devices allows authenticated administrators connected to the local network to tamper with the system.

Severity: MEDIUM (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FR%3AU%2FV%3AD%2FRE%3AL%2FU%3A%2FAmber>)

Acknowledgments: byte\_blaster

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product | Fixed Version |
|---------|---------------|
| CBR750  | v4.6.14.4     |
| EX6120* | EOS           |
| EX6130* | EOS           |
| MR60    | V1.1.7.128    |
| MR70    | V1.0.3.28     |
| MR80    | V1.1.7.6      |
| MS60    | V1.1.7.128    |
| MS70    | V1.0.3.28     |
| MS80    | V1.1.7.6      |
| RAX15*  | EOS           |
| RAX20*  | EOS           |
| RAX200* | EOS           |
| RAX35v2 | V1.0.11.112   |
| RAX38v2 | V1.0.11.112   |

| Product | Fixed Version                                                                                                                  |
|---------|--------------------------------------------------------------------------------------------------------------------------------|
| RAX40v2 | V1.0.11.112                                                                                                                    |
| RAX42*  | V1.0.11.112                                                                                                                    |
| RAX43*  | V1.0.11.112                                                                                                                    |
| RAX45*  | V1.0.11.112                                                                                                                    |
| RAX48   | V1.0.11.112                                                                                                                    |
| RAX50   | V1.0.11.112                                                                                                                    |
| RAX50S  | V1.0.11.112                                                                                                                    |
| RAX75*  | EOS                                                                                                                            |
| RAX80*  | EOS                                                                                                                            |
| RAXE450 | V1.0.10.86                                                                                                                     |
| RAXE500 | V1.0.10.86                                                                                                                     |
| RBR750  | V4.6.14.3                                                                                                                      |
| RBR840* | V4.6.14.3                                                                                                                      |
| RBR850  | V4.6.14.3                                                                                                                      |
| RBRE960 | V6.3.7.5                                                                                                                       |
| RBS750  | V4.6.14.3                                                                                                                      |
| RBS840* | V4.6.14.3                                                                                                                      |
| RBS850  | V4.6.14.3                                                                                                                      |
| RBSE960 | V6.3.7.5                                                                                                                       |
| RS700   | <u>V1.0.7.66 (<a href="https://www.netgear.com/support/product/rs700/">https://www.netgear.com/support/product/rs700/</a>)</u> |
| XR1000  | v1.0.0.68                                                                                                                      |

\* Model has reached its End-of-Support phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

Affected Products



**RBE97x** (<https://www.netgear.com/support/product/RBE97x>) **RBR750** (<https://www.netgear.com/support/product/rbr750/>)



**RBR840** (<https://www.netgear.com/support/product/rbr840/>) **RBR850** (<https://www.netgear.com/support/product/rbr850/>)



**RBR860** (<https://www.netgear.com/support/product/rbr860/>) **RBRE950** (<https://www.netgear.com/support/product/rbre950/>)



**RBRE960** (<https://www.netgear.com/support/product/rbre960/>), **RBS750** (<https://www.netgear.com/support/product/rbs750/>)



**RBS840** (<https://www.netgear.com/support/product/rbs840/>), **RBS850** (<https://www.netgear.com/support/product/rbs850/>)



**RBS860** (<https://www.netgear.com/support/product/rbs860/>) **RBSE950** (<https://www.netgear.com/support/product/rbse950/>)



**RBSE960** (<https://www.netgear.com/support/product/rbse960/>)

**CVE-2026-0415 Insufficient input validation vulnerability in certain Orbi routers**

Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.

Severity: **MEDIUM** (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU>)

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product | Fixed Version                                                                                                              |
|---------|----------------------------------------------------------------------------------------------------------------------------|
| RBE97x  | V9.12.4.9                                                                                                                  |
| RBR750  | <a href="https://www.netgear.com/support/product/rbr750/">V7.2.8.5 (https://www.netgear.com/support/product/rbr750/)</a>   |
| RBR840* | <a href="https://www.netgear.com/support/product/rbr840/">V7.2.8.5 (https://www.netgear.com/support/product/rbr840/)</a>   |
| RBR850  | <a href="https://www.netgear.com/support/product/rbr850/">V7.2.8.5 (https://www.netgear.com/support/product/rbr850/)</a>   |
| RBR860  | <a href="https://www.netgear.com/support/product/rbr860/">V7.2.8.5 (https://www.netgear.com/support/product/rbr860/)</a>   |
| RBRE950 | <a href="https://www.netgear.com/support/product/rbre950/">V7.2.8.5 (https://www.netgear.com/support/product/rbre950/)</a> |
| RBRE960 | <a href="https://www.netgear.com/support/product/rbre960/">V7.2.8.5 (https://www.netgear.com/support/product/rbre960/)</a> |
| RBS750  | <a href="https://www.netgear.com/support/product/rbs750/">V7.2.8.5 (https://www.netgear.com/support/product/rbs750/)</a>   |
| RBS840* | <a href="https://www.netgear.com/support/product/rbs840/">V7.2.8.5 (https://www.netgear.com/support/product/rbs840/)</a>   |

| Product | Fixed Version                                                                                                                |
|---------|------------------------------------------------------------------------------------------------------------------------------|
| RBS850  | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbs850/">https://www.netgear.com/support/product/rbs850/</a> )   |
| RBS860  | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbs860/">https://www.netgear.com/support/product/rbs860/</a> )   |
| RBSE950 | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbse950/">https://www.netgear.com/support/product/rbse950/</a> ) |
| RBSE960 | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbse960/">https://www.netgear.com/support/product/rbse960/</a> ) |

\* Model has reached its End-of-Support phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

Affected Products



**RBE97x** (<https://www.netgear.com/support/product/RBE97x>)

CVE-2026-0414 Arbitrary Code Execution vulnerability exists in RBE970

Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.

Severity: **MEDIUM** (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU>)

Recommendation

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product | Fixed Version |
|---------|---------------|
| RBE97x  | V9.12.4.9     |

Affected Products



**RBE37X** (<https://www.netgear.com/support/product/RBE37X>) **RBE77X** (<https://www.netgear.com/support/product/RBE77X>)



**RBR750** (<https://www.netgear.com/support/product/rbr750/>) **RBR840** (<https://www.netgear.com/support/product/rbr840/>)



**RBR850** (<https://www.netgear.com/support/product/rbr850/>) **RBR860** (<https://www.netgear.com/support/product/rbr860/>)



**RBE950** (<https://www.netgear.com/support/product/rbre950/>).



**RBE960** (<https://www.netgear.com/support/product/rbre960/>), **RBS750** (<https://www.netgear.com/support/product/rbs750/>).



**RBS840** (<https://www.netgear.com/support/product/rbs840/>) **RBS850** (<https://www.netgear.com/support/product/rbs850/>).



**RBS860** (<https://www.netgear.com/support/product/rbs860/>) **RBSE950** (<https://www.netgear.com/support/product/rbse950/>).



**RBSE960** (<https://www.netgear.com/support/product/rbse960/>).

**CVE-2026-0413 Buffer overflow vulnerability in certain NETGEAR Nighthawk routers**

Insufficient input validation of buffers vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.

Severity: MEDIUM (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU>).

Acknowledgments: tmoftf

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product | Fixed Version                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------|
| RBE37X  | V12.1.2.1 ( <a href="https://www.netgear.com/support/product/rbe372/">https://www.netgear.com/support/product/rbe372/</a> )   |
| RBE77X  | V10.5.20.10 ( <a href="https://www.netgear.com/support/product/rbe770/">https://www.netgear.com/support/product/rbe770/</a> ) |
| RBR750  | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbr750/">https://www.netgear.com/support/product/rbr750/</a> )    |
| RBR840* | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbr840/">https://www.netgear.com/support/product/rbr840/</a> )    |
| RBR850  | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbr850/">https://www.netgear.com/support/product/rbr850/</a> )    |
| RBR860  | V7.2.8.5 ( <a href="https://www.netgear.com/support/product/rbr860/">https://www.netgear.com/support/product/rbr860/</a> )    |

\* Model has reached its End-of-Support phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

## A black wireless router with three antennas, positioned at the bottom of the page.

## CVE-2026-0412 Insufficient input validation vulnerability in NETGEAR JR6150 Web UI

This vulnerability has been identified through firmware emulation in a controlled research environment and has not been verified on production hardware.

CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FV%3AD%2FU%3AAmber)

## Recommendation

NETGEAR JR6150 has reached End-of-Support phase, and no further security updates are planned. NETGEAR strongly recommends replacing these devices with newer NETGEAR models to ensure continued security support and updates.

## 18/26



**MR60** (<https://www.netgear.com/support/product/MR60/>) **MR70** (<https://www.netgear.com/support/product/mr70/>)



**MR80** (<https://www.netgear.com/support/product/MR80/>) **MS60** (<https://www.netgear.com/support/product/ms60/>)



**MS70** (<https://www.netgear.com/support/product/ms70/>) **MS80** (<https://www.netgear.com/support/product/ms80/>)



**R6400v2** **R6700v3** **R6900P** (<https://www.netgear.com/support/product/r6900p/>)



**R7000** (<https://www.netgear.com/support/product/r7000/>) **R7000P** (<https://www.netgear.com/support/product/r7000p/>)



**R7960P** (<https://www.netgear.com/support/product/r7960p/>) **R8000P** (<https://www.netgear.com/support/product/r8000p/>)



**R8500** (<https://www.netgear.com/support/product/r8500/>) **RAX20** (<https://www.netgear.com/support/product/rax20/>)



**RAX35v2** (<https://www.netgear.com/support/product/rax35v2/>)



**RAX40v2** (<https://www.netgear.com/support/product/RAX40v2/>) **RAX41** (<https://www.netgear.com/support/product/rax41/>)



**RAX42** (<https://www.netgear.com/support/product/rax42/>) **RAX43** (<https://www.netgear.com/support/product/rax43/>)



**RAX45** (<https://www.netgear.com/support/product/rax45/>) **RAX48** (<https://www.netgear.com/support/product/RAX48/>)



**RAX50** (<https://www.netgear.com/support/product/rax50/>) **RAX50S** (<https://www.netgear.com/support/product/RAX50S/>)



**RAXE450** (<https://www.netgear.com/support/product/raxe450/>)



**RAXE500** (<https://www.netgear.com/support/product/raxe500/>) **XR1000** (<https://www.netgear.com/support/product/xr1000/>)

**CVE-2026-0417 Insufficient input validation in certain NETGEAR routers**

Insufficient input validation vulnerability in NETGEAR devices allows authenticated administrators connected to the local network to tamper with the router's integrity.

Severity: **MEDIUM** (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FV%3AD%2FRE%3AL%2FU%3A%2FAmber>)

Acknowledgments: pjqwudi

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product | Fixed Version |
|---------|---------------|
| MR60    | V1.1.7.132    |
| MR70    | V1.0.3.28     |
| MR80    | V1.1.7.14     |
| MS60    | V1.1.7.132    |

| Product  | Fixed Version                                                                                                             |
|----------|---------------------------------------------------------------------------------------------------------------------------|
| MS70     | V1.0.3.28                                                                                                                 |
| MS80     | V1.1.7.14                                                                                                                 |
| R6400v2* | V1.0.4.128                                                                                                                |
| R6700v3* | V1.0.4.128                                                                                                                |
| R6900P*  | V1.3.3.152                                                                                                                |
| R7000*   | V1.0.11.216                                                                                                               |
| R7000P*  | V1.3.3.152                                                                                                                |
| R7960P*  | V1.4.4.92                                                                                                                 |
| R8000P*  | V1.4.4.92                                                                                                                 |
| R8500*   | EOS                                                                                                                       |
| RAX20*   | <a href="https://www.netgear.com/support/product/rax20/">V1.0.18.144 (https://www.netgear.com/support/product/rax20/)</a> |
| RAX35v2  | V1.0.12.118                                                                                                               |
| RAX40v2  | V1.0.12.118                                                                                                               |
| RAX41*   | V1.0.12.118                                                                                                               |
| RAX42*   | V1.0.12.118                                                                                                               |
| RAX43*   | V1.0.12.120                                                                                                               |
| RAX45*   | V1.0.12.118                                                                                                               |
| RAX48    | V1.0.12.118                                                                                                               |
| RAX50    | V1.0.12.120                                                                                                               |
| RAX50S   | V1.0.12.120                                                                                                               |
| RAXE450  | V1.0.10.86                                                                                                                |
| RAXE500  | V1.0.10.86                                                                                                                |
| XR1000   | V1.0.0.68                                                                                                                 |

\* Model has reached its End-of-Support phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

Affected Products



**RAXE450** (<https://www.netgear.com/support/product/raxe450/>)



**RAXE500** (<https://www.netgear.com/support/product/raxe500/>)

**CVE-2026-0416 RAXE450 and RAXE500 routers allow administrators to modify router functionality beyond intended limits**  
Authenticated administrators connected to the local network can modify router functionality beyond what is intended through the standard management interface.

CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FV%3AD%2FRE%3AL%2FU%3AAMber)

## Recommendation

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

|         |                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------|
| Product | Fixed Version                                                                                                                 |
| RAXE450 | <a href="https://www.netgear.com/support/product/raxe450/">V1.2.14.114 (https://www.netgear.com/support/product/raxe450/)</a> |
| RAXE500 | <a href="https://www.netgear.com/support/product/raxe500/">V1.2.14.114 (https://www.netgear.com/support/product/raxe500/)</a> |

## Affected Products



**RBE97x** (<https://www.netgear.com/support/product/RBE97x>) **RBR350** (<https://www.netgear.com/support/product/rbr350/>)



**RBR760** (<https://www.netgear.com/support/product/RBR760>) **RBS350** (<https://www.netgear.com/support/product/rbs350/>)



**RBS760** (<https://www.netgear.com/support/product/rbs760/>)

## CVE-2026-0411 A Sensitive Information Disclosure Vulnerability in NETGEAR Orbi Satellites

An information disclosure vulnerability in the NETGEAR Orbi satellites could allow a user connected to your network to gain administrator access to the Orbi router. The listed NETGEAR models are affected by this vulnerability.

Orbi WiFi Systems without satellite devices are not impacted by this issue.

CVSS%3A4.0%2FAV%3AA%2FAC%3AL%2FAT%3AP%2FPR%3AL%2FUI%3AN%2FVC%3AH%2FVI%3AN%2FVA%3AN%2FSC%3AH%2FSI%3AH%2FSA%3AH%2FE%3AU)

## Recommendation

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

|         |                                                                                                                                    |
|---------|------------------------------------------------------------------------------------------------------------------------------------|
| Product | Fixed Version                                                                                                                      |
| RBE97x  | V6.3.8.11                                                                                                                          |
| RBR350  | <u>V4.4.2.2</u> ( <a href="https://www.netgear.com/support/product/rbr350/">https://www.netgear.com/support/product/rbr350/</a> )  |
| RBR760  | <u>V6.3.8.11</u> ( <a href="https://www.netgear.com/support/product/rbr760/">https://www.netgear.com/support/product/rbr760/</a> ) |

| Product | Fixed Version                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------|
| RBS350  | V4.4.2.2 ( <a href="https://www.netgear.com/support/product/rbs350/">https://www.netgear.com/support/product/rbs350/</a> )  |
| RBS760  | V6.3.8.11 ( <a href="https://www.netgear.com/support/product/rbs760/">https://www.netgear.com/support/product/rbs760/</a> ) |

Affected Products



**R7000** (<https://www.netgear.com/support/product/r7000/>) **RAX20** (<https://www.netgear.com/support/product/rax20/>)



**RAX35v2** (<https://www.netgear.com/support/product/rax35v2/>) **RAX41** (<https://www.netgear.com/support/product/rax41/>)



**RAX41v2** (<https://www.netgear.com/support/product/rax41v2/>) **RAX42** (<https://www.netgear.com/support/product/rax42/>)



**RAX42v2** (<https://www.netgear.com/support/product/rax42v2/>) **RAX43** (<https://www.netgear.com/support/product/rax43/>)



**RAX43v2** (<https://www.netgear.com/support/product/rax43v2/>) **RAX45** (<https://www.netgear.com/support/product/rax45/>)



**RAX49S** (<https://www.netgear.com/support/product/rax49s/>) **RAX50** (<https://www.netgear.com/support/product/rax50/>)



**RAX50S** (<https://www.netgear.com/support/product/RAX50S/>) **RAX50v2** (<https://www.netgear.com/support/product/rax50v2/>)



**RAX54Sv2** (<https://www.netgear.com/support/product/rax54sv2/>)



**RAX54v2** (<https://www.netgear.com/support/product/RAX54v2/>)



**RAXE450** (<https://www.netgear.com/support/product/raxe450/>)



**RAXE500** (<https://www.netgear.com/support/product/raxe500/>) **XR1000** (<https://www.netgear.com/support/product/xr1000/>)



**XR1000v2** (<https://www.netgear.com/support/product/xr1000v2/>)

**CVE-2026-0410 Insufficient input validation in certain NETGEAR routers**

Authenticated administrators connected to the local network can gain elevated access to the router and make unauthorized changes to router software and functionality.

Severity: **LOW** (<https://www.vulnogram.org/cvss4?CVSS%3A4.0%2FAV%3AA%2FAC%3AH%2FAT%3AN%2FPR%3AH%2FUI%3AN%2FVC%3AN%2FVI%3AH%2FVA%3AN%2FSC%3AN%2FSI%3AN%2FSA%3AN%2FE%3AU%2FV%3AD%2FRE%3AL%2FU%3A%2FAmber>)

Acknowledgments: SmallS

**Recommendation**

NETGEAR strongly recommends that you install the latest firmware as soon as possible.

Issue fixed in:

| Product | Fixed Version                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------|
| R7000*  | V1.0.11.216                                                                                                                 |
| RAX20*  | V1.0.18.144 ( <a href="https://www.netgear.com/support/product/rax20/">https://www.netgear.com/support/product/rax20/</a> ) |
| RAX35v2 | V1.0.16.132                                                                                                                 |
| RAX41*  | V1.0.16.132                                                                                                                 |
| RAX41v2 | V1.1.4.28                                                                                                                   |
| RAX42*  | V1.0.16.132                                                                                                                 |
| RAX42v2 | V1.1.4.28                                                                                                                   |
| RAX43*  | V1.0.16.132                                                                                                                 |
| RAX43v2 | V1.1.4.28                                                                                                                   |
| RAX45*  | V1.0.16.132                                                                                                                 |
| RAX49S  | V1.1.4.28                                                                                                                   |

| Product  | Fixed Version                                                                                                                 |
|----------|-------------------------------------------------------------------------------------------------------------------------------|
| RAX50    | V1.0.16.132                                                                                                                   |
| RAX50S   | V1.0.16.132                                                                                                                   |
| RAX50v2  | V1.1.4.28                                                                                                                     |
| RAX54Sv2 | V1.1.4.28                                                                                                                     |
| RAX54v2  | V1.1.4.28                                                                                                                     |
| RAXE450  | <a href="https://www.netgear.com/support/product/raxe450/">V1.2.14.114 (https://www.netgear.com/support/product/raxe450/)</a> |
| RAXE500  | <a href="https://www.netgear.com/support/product/raxe500/">V1.2.14.114 (https://www.netgear.com/support/product/raxe500/)</a> |
| XR1000   | <a href="https://www.netgear.com/support/product/xr1000/">V1.1.0.22 (https://www.netgear.com/support/product/xr1000/)</a>     |
| XR1000v2 | <a href="https://www.netgear.com/support/product/xr1000v2/">V1.1.0.22 (https://www.netgear.com/support/product/xr1000v2/)</a> |

\* Model has reached its End-of-Support phase and no future security updates are planned. NETGEAR strongly recommends that you retire this device and upgrade to a newer NETGEAR product for continued security support.

**Disclaimer** This document is provided on an "as is" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Your use of the information in the document or materials linked to the document is at your own risk. NETGEAR reserves the right to change or update this document at any time. NETGEAR expects to update this document as new information becomes available.

The above-listed vulnerabilities remain if you do not complete all recommended steps. NETGEAR is not responsible for any consequences that could have been avoided by following the recommendations in this notification.

Last Updated:06/09/2026 | Article ID: 000070811

Was this article helpful?



This article applies to:

- [WiFi 6 \(47\)](#)
- [WiFi 5 \(Wireless AC\) \(26\)](#)
- [Orbi Cellular \(2\)](#)
- [Nighthawk Mesh Systems \(6\)](#)
- [Orbi Cable \(1\)](#)
- [Gaming Routers \(4\)](#)
- [WiFi 7 \(22\)](#)
- [WiFi 6E \(9\)](#)

Recently Viewed Articles

Our team is here to help!

Sign up for news, offers & receive 10% off your first purchase.

Email Address

Submit

<https://github.com/Netgear/netgear/>

United States (English)  

## Enterprise

(<https://www.netgear.com/support/enterprise>)

(<https://www.netgear.com/support/enterprise>)

(<https://www.netgear.com/business/solution-center/business-program/>)

/) (<https://downloads1.netgear.com/files/netg>

Find a Partner/Site-  
(<https://partners.netgear.com/>)

(<https://www.netgear.com/about/legal/>)

Security Advisories (<https://www.netgear.com/about/security/>)

Privacy Policy (<https://www.netgear.com/about/privacy-policy/>)

Ads & Cookie Policy (<https://www.netgear.com/about/ad-cookie-policy/>)

Terms & Conditions (<https://www.netgear.com/about/terms-and-conditions/>)

Accessibility (<https://www.netgear.com/about/accessibility/>)

©1996-2026 NETGEAR®