



# CVE-2021-40866

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2021-40866   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2021-09-13 08:15:00 UTC  |
| <b>Updated</b>         | 2023-08-08 14:22:00 UTC  |
| <b>Description</b>     | Certain NETGEAR smart switches are affected by a remote admin password change by an unauthenticated attacker via the |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                  | Product           | Version | Update | Edition | Language |
|------------------|-------------------------|-------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Netgear</a> | Gc108p            | -       | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gc108pp           | -       | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gc108pp Firmware  | All     | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gc108p Firmware   | All     | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gs108t            | v3      | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gs108tv3          | -       | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gs108t Firmware   | All     | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gs110tp           | v3      | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gs110tpp          | -       | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gs110tpp Firmware | All     | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gs110tp Firmware  | All     | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gs110tup          | -       | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gs110tup Firmware | All     | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gs308t            | -       | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gs308t Firmware   | All     | All    | All     | All      |
| Hardware         | <a href="#">Netgear</a> | Gs310tp           | -       | All    | All     | All      |
| Operating System | <a href="#">Netgear</a> | Gs310tp Firmware  | All     | All    | All     | All      |

|                  |                         |                                    |     |     |     |     |
|------------------|-------------------------|------------------------------------|-----|-----|-----|-----|
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs710tup</a>           | -   | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs710tup Firmware</a>  | All | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs716tp</a>            | -   | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs716tpp</a>           | -   | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs716tpp Firmware</a>  | All | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs716tp Firmware</a>   | All | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs724tp</a>            | v2  | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs724tpp</a>           | -   | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs724tpp Firmware</a>  | All | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs724tp Firmware</a>   | All | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs728tp</a>            | v2  | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs728tpp</a>           | v2  | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs728tpp Firmware</a>  | All | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs728tp Firmware</a>   | All | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs750e</a>             | -   | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs750e Firmware</a>    | All | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs752tp</a>            | v2  | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Gs752tpp</a>           | -   | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs752tpp Firmware</a>  | All | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Gs752tp Firmware</a>   | All | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Ms510txm</a>           | -   | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Ms510txm Firmware</a>  | All | All | All | All |
| Hardware         | <a href="#">Netgear</a> | <a href="#">Ms510txup</a>          | -   | All | All | All |
| Operating System | <a href="#">Netgear</a> | <a href="#">Ms510txup Firmware</a> | All | All | All | All |

## References

### Reference

[Security Advisory for Multiple Vulnerabilities on Some Smart Switches, PSV-2021-0140, PSV-2021-0144, PSV-2021-0145 | Answer | NETGEAR](#)

[Demon's Cries vulnerability \(some NETGEAR smart switches\) - gynvael.coldwind//vx.log](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**