



# CVE-2021-3031

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-3031   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | psirt@paloaltonetworks.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2021-01-13 18:15:00 UTC   |
| <b>Updated</b>         | 2022-10-27 12:51:00 UTC   |
| <b>Description</b>     | Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series |

## Risk And Classification

**Problem Types:** CWE-212

## NVD Known Affected Configurations (CPE 2.3)

| Type     | Vendor                           | Product                 | Version | Update | Edition | Language |
|----------|----------------------------------|-------------------------|---------|--------|---------|----------|
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-200</a>  | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-200</a>  | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-200</a>  | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-2020</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-2020</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-2020</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-2050</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-2050</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-2050</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-220</a>  | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-220</a>  | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-220</a>  | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3020</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3020</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3020</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3050</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3050</a> | -       | All    | All     | All      |

|                  |                                  |                         |     |     |     |     |
|------------------|----------------------------------|-------------------------|-----|-----|-----|-----|
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3050</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3060</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3060</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3060</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3220</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3220</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3220</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3250</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3250</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3250</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3250</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3260</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3260</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-3260</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-500</a>  | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-500</a>  | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-500</a>  | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-5200</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-5200</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-5200</a> | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-800</a>  | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-800</a>  | -   | All | All | All |
| Hardware         | <a href="#">Paloaltonetworks</a> | <a href="#">Pa-800</a>  | -   | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a>  | All | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a>  | All | All | All | All |

## References

| Reference  | Source  | Link  |
|--|---------|---|
| CVE-2021-3031 PAN-OS: Information exposure in Ethernet data frame construction (Etherleak) | CONFIRM | <a href="https://security.paloaltonetworks.com">security.paloaltonetworks.com</a> |
| CVE Program record   | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                                     |
| NVD vulnerability detail   | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                                   |

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** This issue was found by a customer of Palo Alto Networks during a security review.

610383 Google Android November 2021 Security Patch Missing for LGE

© [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](#)