



CVE-2020-14971

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-14971 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-06-23 14:15:00 UTC |
| Updated | 2021-07-21 11:39:00 UTC |
| Description | Pi-hole through 5.0 allows code injection in piholedhcp (the Static DHCP Leases section) by modifying Teleporter backup fil |

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Pi-hole | Pi-hole | All | All | All | All |

References

Reference

- Telspace Systems, The Blog: Pi-hole Code Injection – CVE-2020-14971– Story Time
- missed one (yes yes this can all be squashed) · pi-hole/AdminLTE@8f6e136 · GitHub
- make use of utils.escapeHtml on the JS side of things, and html_entit... · pi-hole/AdminLTE@c949516 · GitHub
- Prevent possible XSS attack vector in the input fields of the group section by PromoFaux · Pull Request #1443 · pi-hole/AdminLTE · GitHub
- 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.

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](#)