



# CVE-2019-12002

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

## Summary

|                        |                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2019-12002                                                                                                        |
| <b>State</b>           | PUBLIC                                                                                                                |
| <b>Assigner</b>        | security-alert@hpe.com                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                          |
| <b>Published</b>       | 2020-04-17 14:15:00 UTC                                                                                               |
| <b>Updated</b>         | 2020-04-28 14:57:00 UTC                                                                                               |
| <b>Description</b>     | A remote session reuse vulnerability leading to access restriction bypass was discovered in HPE MSA 2040 SAN Storage; |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor              | Product                           | Version | Update | Edition | Language |
|------------------|---------------------|-----------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 1040</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 1040</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Hpe</a> | <a href="#">Msa 1040 Firmware</a> | All     | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 1050</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 1050</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Hpe</a> | <a href="#">Msa 1050 Firmware</a> | All     | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2040</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2040</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Hpe</a> | <a href="#">Msa 2040 Firmware</a> | All     | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2042</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2042</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Hpe</a> | <a href="#">Msa 2042 Firmware</a> | All     | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2050</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2050</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Hpe</a> | <a href="#">Msa 2050 Firmware</a> | All     | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2052</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Hpe</a> | <a href="#">Msa 2052</a>          | -       | All    | All     | All      |

|                  |                     |                                   |     |     |     |     |
|------------------|---------------------|-----------------------------------|-----|-----|-----|-----|
| Operating System | <a href="#">Hpe</a> | <a href="#">Msa 2052 Firmware</a> | All | All | All | All |
|------------------|---------------------|-----------------------------------|-----|-----|-----|-----|

## References

| Reference                             | Source  | Link                                                  | Tags                |
|---------------------------------------|---------|-------------------------------------------------------|---------------------|
| Document Display   HPE Support Center | MISC    | <a href="https://support.hpe.com">support.hpe.com</a> | Vendor Advisory     |
| CVE Program record                    | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>         | canonical           |
| NVD vulnerability detail              | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>       | canonical, analysis |

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)