



# CVE-2019-11994

Published on: 01/03/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:36 PM UTC

## CVE-2019-11994

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Simplivity 2600 Gen10](#) from [Hp](#) contain the following vulnerability:

A security vulnerability has been identified in HPE SimpliVity 380 Gen 9, HPE SimpliVity 380 Gen 10, HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen 10, SimpliVity OmniCube, SimpliVity OmniStack for Cisco, SimpliVity OmniStack for Lenovo and SimpliVity OmniStack for Dell nodes. An API is used to execute a command manifest file

during upgrade does not correctly prevent directory traversal and so can be used to execute manifest files in arbitrary locations on the node. The API does not require user authentication and is accessible over the management network, resulting in the potential for unauthenticated remote execution of manifest files. For all customers running HPE OmniStack version 3.7.9 and earlier. HPE recommends upgrading the OmniStack software to version 3.7.10 or later, which contains a permanent resolution. Customers and partners who can upgrade to 3.7.10 should upgrade at the earliest convenience. For all customers and partners unable to upgrade their environments to the recommended version 3.7.10, HPE has created a Temporary Workaround [https://support.hpe.com/hpsc/doc/public/display?](https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=mmr_sf-EN_US000061901&withFrame)

[docLocale=en\\_US&docId=mmr\\_sf-EN\\_US000061901&withFrame](https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=mmr_sf-EN_US000061901&withFrame) for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.

CVE-2019-11994 has been assigned by [security-alert@hpe.com](mailto:security-alert@hpe.com) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| NETWORK                | LOW               | NONE                |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| PARTIAL                | PARTIAL           | PARTIAL             |

CVE References

| Description                           | Tags                                                                                            | Link                                                                                                            |
|---------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Document Display   HPE Support Center | <a href="#">Vendor Advisory</a><br><a href="#">support.hpe.com</a><br><a href="#">text/html</a> | <a href="#">MISC support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=emr_na-hpesbst03956en_us</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                                                         | Vendor             | Product                                         | Version | Update | Edition | Language |
|----------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------|---------|--------|---------|----------|
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 2600 Gen10</a>           | -       | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 2600 Gen10</a>           | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Hp</a> | <a href="#">Simplivity 2600 Gen10 Firmware</a>  | All     | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen10</a>            | -       | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen10</a>            | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen10 Firmware</a>   | All     | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen10 G</a>          | -       | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen10 G</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen10 G Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen9</a>             | -       | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen9</a>             | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Hp</a> | <a href="#">Simplivity 380 Gen9 Firmware</a>    | All     | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity Omnicube</a>             | -       | All    | All     | All      |
| Hardware  | <a href="#">Hp</a> | <a href="#">Simplivity Omnicube</a>             | -       | All    | All     | All      |

|                                                                                            |    |                                          |     |     |     |     |
|--------------------------------------------------------------------------------------------|----|------------------------------------------|-----|-----|-----|-----|
| Operating System                                                                           | Hp | Simplivity Omnicube Firmware             | All | All | All | All |
| Hardware  | Hp | Simplivity Omnistack For Cisco           | -   | All | All | All |
| Hardware  | Hp | Simplivity Omnistack For Cisco           | -   | All | All | All |
| Operating System                                                                           | Hp | Simplivity Omnistack For Cisco Firmware  | All | All | All | All |
| Hardware  | Hp | Simplivity Omnistack For Dell            | -   | All | All | All |
| Hardware  | Hp | Simplivity Omnistack For Dell            | -   | All | All | All |
| Operating System                                                                           | Hp | Simplivity Omnistack For Dell Firmware   | All | All | All | All |
| Hardware  | Hp | Simplivity Omnistack For Lenovo          | -   | All | All | All |
| Hardware  | Hp | Simplivity Omnistack For Lenovo          | -   | All | All | All |
| Operating System                                                                           | Hp | Simplivity Omnistack For Lenovo Firmware | All | All | All | All |
| cpe:2.3:h:hp:simplivity_2600_gen10:-:*:*:*:*:*:                                            |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_2600_gen10:-:*:*:*:*:*:                                            |    |                                          |     |     |     |     |
| cpe:2.3:o:hp:simplivity_2600_gen10_firmware:*:*:*:*:*:                                     |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_380_gen10:-:*:*:*:*:*:                                             |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_380_gen10:-:*:*:*:*:*:                                             |    |                                          |     |     |     |     |
| cpe:2.3:o:hp:simplivity_380_gen10_firmware:*:*:*:*:*:                                      |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_380_gen10_g:-:*:*:*:*:*:                                           |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_380_gen10_g:-:*:*:*:*:*:                                           |    |                                          |     |     |     |     |
| cpe:2.3:o:hp:simplivity_380_gen10_g_firmware:*:*:*:*:*:                                    |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_380_gen9:-:*:*:*:*:*:                                              |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_380_gen9:-:*:*:*:*:*:                                              |    |                                          |     |     |     |     |
| cpe:2.3:o:hp:simplivity_380_gen9_firmware:*:*:*:*:*:                                       |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_omnicube:-:*:*:*:*:*:                                              |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_omnicube:-:*:*:*:*:*:                                              |    |                                          |     |     |     |     |
| cpe:2.3:o:hp:simplivity_omnicube_firmware:*:*:*:*:*:                                       |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_omnistack_for_cisco:-:*:*:*:*:*:                                   |    |                                          |     |     |     |     |
| cpe:2.3:h:hp:simplivity_omnistack_for_cisco:-:*:*:*:*:*:                                   |    |                                          |     |     |     |     |
| cpe:2.3:o:hp:simplivity_omnistack_for_cisco_firmware:*:*:*:*:*:                            |    |                                          |     |     |     |     |

```
cpe:2.3:h:hp:simplivity_omnistack_for_dell:-:*:*:*:*:*:
```

```
cpe:2.3:h:hp:simplivity_omnistack_for_dell:-:*:*:*:*:*:
```

cpe:2.3:o:hp:simplivity\_omnistack\_for\_dell\_firmware:\*:\*:\*:\*:\*:

```
cpe:2.3:h:hp:simplivity_omnistack_for_lenovo:-.*:.*:.*:.*:.*:
```

```
cpe:2.3:h:hp:simplivity_omnistack_for_lenovo:-:*:*:*:*:*:
```

```
cpe:2.3:o:hp:simplivity_omnistack_for_lenovo_firmware:*.*.*.*.*.*.*.*.*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

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](https://status.cve.report)