

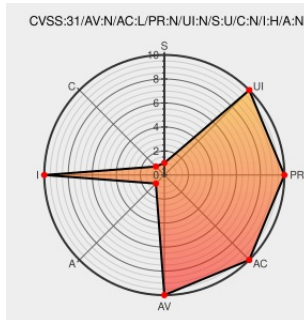


CVE-2019-11993

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

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

CVE-2019-11993

[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. Two now deprecated APIs run as root, accept a file

name path, and can be used to create or delete arbitrary files on the nodes. These APIs do not require user authentication and are accessible over the management network, resulting in remote availability and integrity vulnerabilities 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?docLocale=en_US&docId=mmr_sf-EN_US000061675&withFrame for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.

CVE-2019-11993 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **9.4 - HIGH**

Access	Access	Authentication
--------	--------	----------------

Vector	Complexity	
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Document Display HPE Support Center	Vendor Advisory support.hpe.com text/html	MISC support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03955en_us

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Hp	Simplivity 2600 Gen10	-	All	All	All
Hardware 	Hp	Simplivity 2600 Gen10	-	All	All	All
Operating System	Hp	Simplivity 2600 Gen10 Firmware	All	All	All	All
Hardware 	Hp	Simplivity 380 Gen10	-	All	All	All
Hardware 	Hp	Simplivity 380 Gen10	-	All	All	All
Operating System	Hp	Simplivity 380 Gen10 Firmware	All	All	All	All
Hardware 	Hp	Simplivity 380 Gen10 G	-	All	All	All
Hardware 	Hp	Simplivity 380 Gen10 G	-	All	All	All
Operating System	Hp	Simplivity 380 Gen10 G Firmware	All	All	All	All
Hardware 	Hp	Simplivity 380 Gen9	-	All	All	All
Hardware 	Hp	Simplivity 380 Gen9	-	All	All	All
Operating System	Hp	Simplivity 380 Gen9 Firmware	All	All	All	All
Hardware 	Hp	Simplivity Omnicube	-	All	All	All
Hardware 	Hp	Simplivity Omnicube	-	All	All	All
Operating System	Hp	Simplivity Omnicube Firmware	All	All	All	All

۷۹۵۰۰۰

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_omnystack_for_dell:-:*:*:*:*:*:
cpe:2.3:o:hp:simplivity_omnystack_for_dell_firmware:*:*:*:*:*:
cpe:2.3:h:hp:simplivity_omnystack_for_lenovo:-:*:*:*:*:*:
cpe:2.3:h:hp:simplivity_omnystack_for_lenovo:-:*:*:*:*:*:
cpe:2.3:o:hp:simplivity_omnystack_for_lenovo_firmware:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)