Migration Specialties International, Inc.
217 West 2nd Street, Florence, CO 81226-1403
+1 719-784-9196
E-mail: *Info@MigrationSpecialties.com*
www.MigrationSpecialties.com

Continuity in Computing

OpenVMS Command Definition Utility Vulnerability Mitigation: V4.0 – V8.4-2L2

February 23, 2018 **CVE-2017-17482**

1. SUMMARY

VAX and Alpha systems running versions of OpenVMS from 4.0 through 8.4-2L2 are susceptible to a Command Definition Utility vulnerability. The vulnerability allows a non-privileged user account to obtain elevated privileges that give it access to secured parts of the system. The vulnerability has been assigned the Common Vulnerabilities and Exposures designation CVE-2017-17482. See this article in *The Register* for additional details:

https://www.theregister.co.uk/2018/02/06/openvms_vulnerability/

To exploit the vulnerability, a hacker must have access to a user account, know how to add a command to the local process DCL table, and know how to create a malformed command that implants the information necessary to elevate command privileges on the non-privileged user process.

Integrity systems are also susceptible to the vulnerability, but are considered a less serious risk because the hack simply crashes the user process rather than allowing elevation of process privileges. To quote from an anonymous HPE source:

> "CVE-2017-17482 is the OpenVMS vulnerability in the Command Definition Utility (CDU). The defect is believed to potentially allow an unprivileged user to elevate privileges. The same defect is present on Integrity; however, the differences in the Itanium architecture prevent the defect from being exploited. Any attempt to gain elevated privileges results in a process crash on Itanium."

2. VULNERABILITY PATCH

If you are running a supported version of OpenVMS, the best solution is to upgrade to OpenVMS 8.4-2 and apply the VSI supplied patch for the CVE-2017-17482 vulnerability.

2.1 VSI OpenVMS Customers

Alpha and Integrity users running VSI OpenVMS can obtain a patch kit from VSI. VSI does not supply VAX versions of OpenVMS. See this link for additional information:

https://groups.google.com/forum/#!topic/comp.os.vms/BYIUQ0lJ-s0

2.2 HPE OpenVMS

Alpha and Integrity users running HPE OpenVMS 8.4-1 and higher with an active HPE support contract can contact HPE to obtain the VSI patch kit.

VAX, Alpha, and Integrity users running HPE OpenVMS 8.4 or lower must contact HPE customer support. These users will have to wait for a DCL ECO release via the HPESC site. As of this writing, no release date has been announced. Monitor the CVE site at this link for updates on the vulnerability status:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17482

3. WORKAROUND

For VAX, Alpha, and Integrity users unable to patch OpenVMS, here are ways to protect your systems from the vulnerability.

- Practice good user account control. A hacker must be able to log into the OpenVMS system to exploit the vulnerability.
- Disable user access to the DCL "SET COMMAND". Most unprivileged users should never need access to this function. As HPE explains:

  The vulnerability is in the CDU.EXE image, which is installed with CMEXEC privilege, and a workaround is to remove privileges from the image. This can be done by editing the files SYS$MANAGER:VMSIMAGES.DAT plus the master VMS$IMAGES_MASTER.DAT and then rebooting.

  The relevant lines look like this (this may vary between versions of OpenVMS):

```
$ search sys$manager:vms$images_master.dat,vmsimages.dat cdu
******************************
SYS$COMMON:[SYSMGR]VMS$IMAGES_MASTER.DAT;1
sys$system:cdu /open /header /priv=(cmexec) !
******************************
SYS$SYSROOT:[SYSMGR]VMSIMAGES.DAT;1
SYS$SYSTEM:CDU /OPEN /HEADER /PRIV=(CMEXEC) ! 1/0/
```

  The workaround would be to simply remove the “/PRIV=(CMEXEC)” qualifier from these lines. This prevents a non-privileged user from using the DCL "SET COMMAND".

- Along the same vein, the system DCL table could be patched to remove the COMMAND option from the SET command.