CERT Advisory CA-1992-18 VMS Monitor Vulnerability

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

CA-92:16                        CERT Advisory
                              September 22, 1992
                          VMS Monitor Vulnerability

- ----------------------------------------------------------------------------
                  *** SUPERSEDED BY CA-92:18 ***

The CERT Coordination Center has received information concerning a
potential vulnerability with Digital Equipment Corporation's VMS
Monitor.  This vulnerability is present in V5.0 through V5.4-2 but has
been corrected in V5.4-3 through V5.5-1.  The Software Security
Response Team at Digital has provided the following information
concerning this vulnerability.

NOTE: Digital suggests that customers who are unable to upgrade their
systems implement the workaround described below.

For additional information, please contact your local Digital Equipment
Corporation customer service representative.


       Beginning of Text provided by Digital Equipment Corporation
==============================================================================
SSRT-0200      PROBLEM: Potential Security Vulnerability Identified in Monitor
                SOURCE: Digital Equipment Corporation
                AUTHOR: Software Security Response Team - U.S.
                        Colorado Springs USA

               PRODUCT:  VMS
Symptoms Identified On:  VMS, Versions 5.0, 5.0-1, 5.0-2, 5.1, 5.1-B,
                                       5.1-1, 5.1-2, 5.2, 5.2-1, 5.3,
                                       5.3-1, 5.3-2, 5.4, 5.4-1, 5.4-2

            ******************************************************
            SOLUTION: This problem is not present in VMS V5.4-3
                      (released in October 1991) through V5.5-1
                      (released in July, 1992.)
            ******************************************************
Copyright (c) Digital Equipment Corporation, 1992 All Rights Reserved.
Published Rights Reserved Under The Copyright Laws Of The United States.
- ----------------------------------------------------------------------------
PROBLEM/IMPACT:
- ----------------------------------------------------------------------------
     Unauthorized privileges may be expanded to authorized users of a system
     under certain conditions, via the Monitor utility.   Should a system be
     compromised through unauthorized access, there is a risk of potential
     damage to a system environment.  This problem will not permit unauthorized
     access entry, as individuals attempting to gain unauthorized access will
     continue to be denied through the standard VMS security mechanisms.
- ----------------------------------------------------------------------------
SOLUTION:
- ----------------------------------------------------------------------------
     This potential vulnerability does not exist in VMS V5.4-3
     (released in October 1991) and later versions of VMS through V5.5-1.

     Digital strongly recommends that you upgrade to a minimum of VMS V5.4-3,
     and further, to the latest release of VMS V5.5-1. (released in July, 1992)
- ----------------------------------------------------------------------------
INFORMATION:
- ----------------------------------------------------------------------------
     If you cannot upgrade at this time Digital recommends that you
     implement a workaround (examples attached below) to avoid any potential
     vulnerability.

     As always, Digital recommends that you periodically review your system
     management and security procedures.  Digital will continue to review and
     enhance the security features of its products and work with customers to
     maintain and improve the security and integrity of their systems.
- ----------------------------------------------------------------------------
WORKAROUND
- ----------------------------------------------------------------------------
     A suggested workaround would be to remove the installed image
     SYS$SHARE:SPISHR.EXE via VMS INSTALL and/or restrict the use of
     the MONITOR utility to "privileged" system administrators.
     Below are the examples of doing both;

[1]  To disable the MONITOR utility the image SYS$SHARE:SPISHR.EXE should be
```

deinstalled.

From a privileged account;

For cluster configurations;

```
$ MC SYSMAN
SYSMAN> SET ENVIRONMENT/CLUSTER
SYSMAN> DO INSTALL REMOVE SYS$SHARE:SPISHR.EXE
SYSMAN> DO RENAME SYS$SHARE:SPISHR.EXE   SPISHR.HOLD
SYSMAN> EXIT
```

For non-VAXcluster configurations;

```
$INSTALL
INSTALL>REMOVE SYS$SHARE:SPISHR.EXE
INSTALL>EXIT
$RENAME SYS$SHARE:SPISHR.EXE SPISHR.HOLD
```

[2] If you wish to restrict access to the MONITOR command so that only a limited number of authorized (or privileged) persons are granted access to the utility, one method might be to issue the following example commands;

From a privileged account;

For cluster configurations;

```
$ MC SYSMAN
SYSMAN> SET ENVIRONMENT/CLUSTER
SYSMAN> DO INSTALL REMOVE SYS$SHARE:SPISHR.EXE
SYSMAN> DO SET FILE/ACL=(ID=*,ACCESS=NONE) SYS$SHARE:SPISHR.EXE
SYSMAN> DO SET FILE/ACL=(ID=SYSTEM,ACCESS=READ+EXECUTE) SYS$SHARE:SPISHR.EXE
SYSMAN> DO INSTALL ADD SYS$SHARE:SPISHR.EXE/OPEN/HEADER/SHARE/PROTECT
SYSMAN> EXIT
$
```

THIS WILL IMPACT the MONITOR UTILITY FOR REMOTE MONITORING.
LOCAL MONITORING WILL CONTINUE TO WORK FOR PERSONS HOLDING THE ID's GRANTED ACL ACCESS.

see additional note(s) below

For non-VAXcluster configurations;

```
$ INSTALL
INSTALL>REMOVE SYS$SHARE:SPISHR.EXE
INSTALL>EXIT
$ SET FILE /ACL=(ID=*,ACCESS=NONE) SYS$SHARE:SPISHR.EXE
$ SET FILE /ACL=(ID=SYSTEM,ACCESS=READ+EXECUTE) SYS$SHARE:SPISHR.EXE
$ INSTALL
INSTALL>ADD SYS$SHARE:SPISHR.EXE/OPEN/HEADER/SHARE/PROTECT
INSTALL>EXIT
$
```

IN THE ABOVE EXAMPLES, THE "SET FILE /ACL" LINE SHOULD BE REPEATED FOR ALL ACCOUNTS THAT ARE REQUIRED/ALLOWED TO USE THE DCL MONITOR COMMAND.

NOTE: The ID -SYSTEM- is an example, and should be substituted as necessary with valid user ID's that are associated with accounts you wish to grant access to.

==========

End of Text provided by Digital Equipment Corporation

- ---

CERT wishes to thank Teun Nijssen of CERT-NL (the SURFnet CERT, in the Netherlands) for bringing this security vulnerability to our attention. We would also like to thank Digital Equipment Corporation's Software Security Response Team for providing information on this vulnerability.

- ---

If you believe that your system has been compromised, contact CERT or your representative in FIRST (Forum of Incident Response and Security Teams).

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
CERT personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4), on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Past advisories, information about FIRST representatives, and other
information related to computer security are available for anonymous ftp
from cert.org (192.88.209.5).

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBOBS9x1r9kb5qlZHQEQLfKwCg3dYLzg7RhIIG08AB0dMd9K3kmI4AnAyr
GZ/0fHR4YaXLBckCzaRshPrl
=wXMo
-----END PGP SIGNATURE-----