CERT Advisory CA-1993-05 OpenVMS and OpenVMS AXP Vulnerability

Original issue date: February 24, 1993
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning a potential vulnerability with Digital Equipment Corporation's OpenVMS and OpenVMS AXP. This vulnerability is present in OpenVMS V5.0 through V5.5-2 and OpenVMS AXP V1.0 but has been corrected in OpenVMS V6.0 and OpenVMS AXP V1.5. The Software Security Response Team at Digital Equipment Corporation has provided the following information concerning this vulnerability.

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

Beginning of Text Provided by Digital Equipment Corporation

```
23.FEB.1993

     SOURCE:            Digital Equipment Corporation
     AUTHOR:            Software Security Response Team
                        Colorado Springs USA

             PRODUCT: OpenVMS V5.0 through V5.5-2 & OpenVMS AXP V1.0

             PROBLEM: Potential Security Vulnerability - OpenVMS

             SOLUTION: A remedial kit is now available for
                       OpenVMS AXP V1.0 and OpenVMS V5.0 through
                       V5.5-2 (including all SEVMS versions V5.1 through
                       V5.5-2 as applicable) by contacting your normal
                       Digital Services Support organization.

             SEVERITY LEVEL: High

     This potential vulnerability has been corrected in the next release of
     OpenVMS V6.0 and OpenVMS AXP V1.5.  For VMS Versions prior to
     OpenVMS V5.0, Digital strongly recommends that you upgrade to a
     minimum of OpenVMS V5.0 and further, to the latest release of
     OpenVMS V5.5-2.

     ------------------------------------------------------------------------
           The remedial kits may be identified as:

                VAXSYS01_U2050   VMS V5.0, V5.0-1, V5.0-2
                VAXSYS01_U1051   VMS V5.1
                VAXSYS01_U1052   VMS V5.2
                VAXSYS01_U2053   VMS V5.3 thru V5.3-2
                VAXSYS01_U3054   VMS V5.4 thru V5.4-3
                VAXSYS02_U2055   OpenVMS V5.5 thru V5.5-2
                AXPSYS01_010     OpenVMS AXP V1.0

     ------------------------------------------------------------------------
     Copyright (c) Digital Equipment Corporation, 1993 All Rights Reserved.
     Published Rights Reserved Under The Copyright Laws Of The United States.

     ------------------------------------------------------------------------
     ADVISORY INFORMATION:
     ------------------------------------------------------------------------

     This update kit corrects a potential security vulnerability in
     the OpenVMS VAX and OpenVMS AXP operating systems.  This potential
     vulnerability may be further exploited in the form of a malicious program
     that may allow authorized but unprivileged users to obtain all system
     privileges, potentially giving the unprivileged user control of your
     OpenVMS system and data.

     NOTE:

     The update kit must be applied if an update or installation is performed
     for all versions prior to OpenVMS V6.0 or OpenVMS AXP V1.5.  For VMS
     Versions prior to OpenVMS V5.0, Digital strongly recommends that
     you upgrade to a minimum of OpenVMS V5.0 and further to the
     latest release of OpenVMS V5.5-2.

     ------------------------------------------------------------------------
```

```
INFORMATION:
-----------------------------------------------------------------------

Digital strongly recommends that you install the available kit on your
system(s), to avoid any potential vulnerability as a result of this
problem.

Customers with a Digital Services contract may obtain a kit for the
affected versions of OpenVMS by contacting your normal support
organizations.

-  In the U.S. Customers may contact the Customer Support Center
   at 1(800)354-9000 and request the appropriate kit for your version
   of OpenVMS, or through DSNlink Text Search database using the
   keyword text "Potential Security Vulnerability", or DSNlink VTX using
   the patch number 1084.

-  Customers in other geographies should contact their normal Digital
   Services support organizations.

As always, Digital recommends you to regularly review your system
management and security procedures.  Digital will continue to review and
enhance security features, and work with our customers to further improve
the integrity of their systems.
```

End of Text Provided by Digital Equipment Corporation

The CERT Coordination Center wishes to thank Digital Equipment Corporation's Software Security Response Team for their response to this problem.

Revision History

```
September 19,1997 Attached Copyright Statement
```