DG SUPPORT NOTICE: Security Bypass Vulnerability with RME

Endpoint DLP

Issue

A security bypass vulnerability exists in the removable media encryption (RME) component of the Digital Guardian Windows Agent prior to version 8.2.0. This allows a user to circumvent encryption controls by modifying metadata on the USB device thereby compromising the confidentiality of future stored data. NOTE: Data already encrypted on the device is unaffected by this change. This relates to CVE-2024-3334.

Resolution

There are two things required to remediate the bypass:
1. Upgrade the Windows Agent to version 8.2.0 or above.
2. Deploy the Windows DLP Control Policy Pack v4.1 and ensure that rule "
DLP1028-P-Verify RME is Active" is enabled or, if you do not use the content pack or use the, now deprecated alternative RME policies, there is a standalone version of the rule "
DLP1028-P-Standalone Verify RME is Active".

For reference the alternative RME policies include the following rules:
DLP - Classified RME USB Enterprise alternative
DLP - Classified RME USB Portable alternative
DLP - Classified RME USB User Decision alternative
DLP - RME USB Enterprise alternative
DLP - RME USB Portable alternative
DLP - RME USB User Decision alternative

An export of the rule is available for import linked to this article as DLP1028-P-Standalone Verify RME is Active.xml
The rule must be set to block or use a block prompt to be effective.

Here is the rule logic for reference:

```
<!--
Rule Logic:
```

```
 <or>
  <and>
   Destination Drive does not support encryption
   Destination Drive is Removable
   Operation is FileCopy, Move or Rename
  </and>
  <and>
   Source path is not in the exceptions list
   Operation is FileCreate or FileWrite
   Source Drive does not support encryption
   Source Drive is Removable
  </and>
</or>
-->

<or>
  <and>
    <!--
    <set>
      <varstring name="DLP1028StandaloneDestPath" scope="event"/>
      <evtDestFilePath/>
    </set>
    -->
    <equal>
      <evtDestSupportsEncrypt/>
      <bool value="false"/>
    </equal>
    <in>
      <evtDestDriveType/>
      <list>
        <constDriveRemovable/>
      </list>
    </in>
    <in>
      <evtOperationType/>
      <list>
        <constOpFileCopy/>
        <constOpFileMove/>
        <constOpFileRename/>
      </list>
    </in>
  </and>
  <and>
    <!--
```

```
  <set>
   <varstring name="DLP1028StandaloneSrcPath" scope="event"/>
   <evtSrcFilePath/>
  </set>
  -->
  <not>
   <in op="like">
    <evtSrcFilePath/>
    <list>
     <string value="%\DG1__DMK_DIR_HDR%"/>
     <string value="%\.DG1__DMK_DIR_HDR%"/>
     <string value="%\:DG1__DMK_DIR_HDR%"/>
     <string value="%\dg1__ds_vol_hdr%"/>
     <string value="%\.dg1__ds_vol_hdr"/>
     <string value="%\:DG1__DS_VOL_CACHE_HDR"/>
     <string value="%\:DG1__DS_VOL_CACHE_HDR"/>
     <string value="%\:DG1__DS_DIR_HDR"/>
     <string value="%\DG1__DS_DIR_HDR"/>
     <string value="%:\system volume information%"/>
     <string value="%:"/>
    </list>
   </in>
  </not>
  <in>
   <evtOperationType/>
   <list>
    <constOpFileCreate/>
    <constOpFileWrite/>
   </list>
  </in>
  <equal>
   <evtSrcSupportsEncrypt/>
   <bool value="false"/>
  </equal>
  <equal>
   <evtSrcDriveType/>
   <constDriveRemovable/>
  </equal>
 </and>
</or>
```

Was this page helpful? 0 0

Still not finding the help you need?

LOG IN CONTACT US