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.


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
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)
Vulnerability 1: 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 Configuration](image)

This page lets you set up Installation Manager configurations, or check for new packages from the Online Support site.
2. Replay following request in BurpSuite with session Cookies removed:

![BurpSuite Request and Response](image_url)

**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 Configuration](image_url)

**Configuration**

This page lets you set up Installation Manager configurations, or check for new packages from the Online Support site.
Vulnerability 2: 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:

![Avamar® Installation Manager Configuration]

2. Replay following request in BurpSuite with session Cookies removed:
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.
Vulnerability 3: 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:

3. Intercept the server response:

4. Change the response to ‘True’ from ‘False’:
5. It unlocks the support account:

6. View the logs:
7. View verbose logs:

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

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.