DSA-2020-039: Dell EMC Isilon OneFS Security Update for a SyncIQ Vulnerability

Dell EMC Identifier: DSA-2020-039

CVE Identifier: CVE-2020-5328

Severity: Critical

Severity Rating: CVSS v3 Base Score: 9.8 (CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected products:
Dell EMC Isilon OneFS versions though OneFS 8.2.2

Summary:

Dell EMC Isilon OneFS 8.2.0 and later contains a workaround for a SyncIQ a vulnerability that affects all current versions of OneFS though OneFS 8.2.2. This vulnerability may potentially be exploited by malicious users to compromise the affected system.

Details:

Dell EMC Isilon OneFS (all current versions) contain an unauthorized access vulnerability due to a lack of thorough authorization checks in SyncIQ. This is only impactful if the SyncIQ feature is licensed, and the encrypted syncs option is not marked as required. When this happens, loss of control of the cluster may occur.

.

Workaround:

Scenario	OneFS versions prior to 8.2.0	OneFS 8.2.0 and later
SyncIQ is not licensed	No change needed	No change needed
SyncIQ is licensed but not used	Disable SyncIQ: 1. On the cluster, log in as SSH. 2. Run the following command to disable SyncIQ: `isi sync settings modify –service=Off`	Disable SyncIQ: 1. On the cluster, log in as SSH. 2. Run the following command to disable SyncIQ: `isi sync settings modify –service=Off`
SyncIQ is licensed and used	1. Upgrade to OneFS 8.2.0 on all clusters that are using SyncIQ. 2. Follow the workaround instructions in **For OneFS versions 8.2.0 and later** in the next cell.	1. Enable SyncIQ encryption for each impacted cluster. For more details, see the **Configure certificates** procedure described in the **Data Encryption with SyncIQ** chapter of the OneFS 8.2.0 CLI Administration Guide, and the steps that need to be run on each policy to enable encryption. 2. Create a SyncIQ policy to enable encryption, as described in the **Create encrypted SyncIQ policies** procedure of the guide. 3. Force SyncIQ encryption, as described in the same procedure. `isi sync setting mod --encryption-required=True`
Adjustment to lessen the vulnerability impact	The cluster can be left in a less vulnerable state by enabling a SyncIQ password. For more information see How to use a PSK when using SyncIQ since 7.0.0 on the Customer support site.	

NOTE: Because SyncIQ encryption requires mutual authentication SSL handshakes, each cluster must specify its own identity certificate and the CA certificate of the peer. For more information, see the SyncIQ traffic encryption section of the OneFS 8.2.1 Web Admin Guide.

Severity Rating

For an explanation of Severity Ratings, refer to Dell EMC Knowledgebase article 468307 (https://support.emc.com/kb/468307). Dell EMC recommends all customers take into account both the base score and any relevant temporal and environmental scores which may impact the potential severity associated with particular security vulnerability.

Legal Information

Read and use the information in this Dell EMC Security Advisory to assist in avoiding any situation that might arise from the problems described herein. If you have any questions regarding this product alert, contact Dell EMC Software Technical Support at 1-877-534-2867.

For an explanation of Severity Ratings, refer to Dell EMC Knowledgebase article 468307. Dell EMC recommends all customers take into account both the base score and any relevant temporal and environmental scores which may impact the potential severity associated with particular security vulnerability.

Read and use the information in this Dell EMC Security Advisory to assist in avoiding any situation that might arise from the problems described herein. If you have any questions regarding this product alert, contact Dell EMC Software Technical Support at 1-877-534-2867. Dell EMC distributes Dell EMC Security Advisories, in order to bring to the attention of users of the affected Dell EMC products, important security information. Dell EMC recommends that all users determine the applicability of this information to their individual situations and take appropriate action. The information set forth herein is provided "as is" without warranty of any kind. Dell EMC disclaims all warranties, either express or implied, including the warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event, shall Dell EMC or its suppliers, be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell EMC or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.