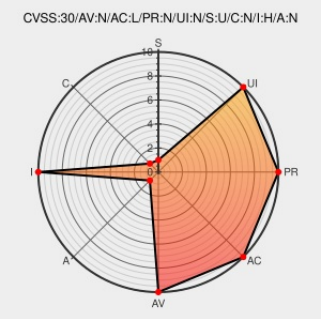
CVE-2018-15766

Published on: 10/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:28 PM UTC

CVE-2018-15766

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Encryption from Dell contain the following vulnerability:

On install, Dell Encryption versions prior 10.0.1 and Dell Endpoint Security Suite Enterprise versions prior 2.0.1 will overwrite and manually set the "Minimum Password Length" group policy object to a value of 1 on that device. This allows for users to bypass any existing policy for password length and potentially create insecure password on their device. This value is defined during the installation of the "Encryption Management Agent" or "EMAgent" application. There are no other known values modified.

CVE-2018-15766 has been assigned by security_alert@emc.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Dell** - **Encryption** version **10.0.1**

Affected Vendor/Software: **Dell** - **Endpoint Security Suite Enterprise** version **2.0.1**

Vulnerability Patch/Work Around

For affected devices, the minimum password length policy should be changed manually to what is desired for the current environment. If Dell Endpoint Security Suite Enterprise or Dell Encryption Enterprise's Encryption Management Agent is installed on a Domain Controller or a device that is not joined to a domain, the default minimum password length will need to be changed on the local device. If Dell Endpoint Security Suite Enterprise or Dell Encryption Enterprise's Encryption Management Agent is installed on a device that is joined to a domain, the default minimum password length will need to be changed within the enterprise's Group Policy Management console. Default values for this property is '7' in most configurations. This Microsoft KB article outlines how to modify this setting: https://technet.microsoft.com/en-us/library/dd277399.aspx External Link

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Dell Encryption and Dell Endpoint Security Suite Enterprise Security Policy Overwrite Vulnerability | Dell US	Mitigation Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.dell.com/support/article/us/en/04/sln313561/dell-encryption-and-dell-endpoint-security-suite-enterprise-security-policy-overwrite-vulnerability?lang=en

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dell	Encryption	All	All	All	All
Application	Dell	Encryption	All	All	All	All
Application	Dell	Endpoint Security Suite Enterprise	All	All	All	All
Application	Dell	Endpoint Security Suite Enterprise	All	All	All	All

cpe:2.3:a:dell:encryption:*:*:*:*:*:*:*:*:

cpe:2.3:a:dell:encryption:*:*:*:*:*:*:*:*:

cpe:2.3:a:dell:endpoint_security_suite_enterprise:*:*:*:*:*:*:*:*:

cpe:2.3:a:dell:endpoint_security_suite_enterprise:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report