Array Networks Security Advisory: Microsoft Credential Security Support Provider Protocol (CredSSP) Vulnerability (CVE-2018-0886)

Advisory Date: May 2, 2018

Overview

Credential Security Support Provider protocol (CredSSP) is an authentication provider that processes authentication requests for other applications.

A remote code execution vulnerability exists in unpatched versions of CredSSP. An attacker who successfully exploits this vulnerability could relay user credentials to execute code on the target system. Any application that depends on CredSSP for authentication may be vulnerable to this type of attack.

Reference:

https://support.microsoft.com/en-us/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018

Impact

Array AG Series' DesktopDirect solution may be affected by this vulnerability when the RDP client uses a vulnerable CredSSP client component and the remote desktop (RDP server) uses a vulnerable CredSSP server component.

Mitigation

Microsoft released a patch on March 13, 2018 to update the CredSSP authentication protocol and the Remote Desktop clients for all affected Windows platforms. In addition, Microsoft has released the Remote Desktop Client 8.1.41.1803231609 for iOS to address this vulnerability.

After this patch is installed, a Group Policy setting called "Encryption Oracle Remediation" (**Computer Configuration -> Administrative Templates -> System -> Credentials Delegation**) is available to control compatibility with vulnerable clients and servers. After setting it to "Force updated clients" or "Mitigated" on client and server computers, this vulnerability can be mitigated.

In addition, Microsoft will release a patch on May 8, 2018 to change the default value of the "Encryption Oracle Remediation" setting from "Vulnerable" to "Mitigated".

Please note that after the patch or a new RDP client is installed, remote desktop access may be affected by the setting of “Encryption Oracle Remediation”. The following table describes the test results from Array Networks’s lab.

RDP Client Setting		**RDP Server Setting**			
		Unpatched	**Force updated clients**	**Mitigated**	**Vulnerable**
Windows	**Unpatched**	Allowed	Blocked	Allowed	Allowed
	Force updated clients	Blocked	Allowed	Allowed	Allowed
	Mitigated	Blocked	Allowed	Allowed	Allowed
	Vulnerable	Allowed	Allowed	Allowed	Allowed
MacOS	**No patch**	Allowed	Blocked	Allowed	Allowed
iOS	**No patch**	Allowed	Blocked	Allowed	Allowed
	Microsoft Remote Desktop Client 8.1.41.1803231609	Allowed	Allowed	Allowed	Allowed
Android	**No patch**	Allowed	Blocked	Allowed	Allowed

In conclusion, Array Networks recommends that you install the latest patch on computers that host the RDP clients and function as RDP severs, and set “Encryption Oracle Remediation” to “Mitigated”.