Security Notification – WannaCry Ransomware Attack

15-May-2017

Overview

Starting early Friday morning on May 12th, ransomware attacks using the Eternal Blue exploit for Microsoft windows were executed across businesses in hundreds of countries. The attacks locked down businesses in users across industries like telecommunications and healthcare. This new ransomware variant known as WannaCry, WCry, WannaCrypt, or Wanna Decryptor, targets and exploits a Windows SMBv1 vulnerability that was patched by Microsoft® in March in security bulletin MS17-010. Other infection vectors include Remote Desktop Protocol (RDP) compromise and phishing emails.

Vulnerability Overview

The vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

Product(s) Affected

Customers using Microsoft® Windows operating systems.

Vulnerability Details

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server. To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server. The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

- **Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143**
- **Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144**
- **Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145**
- **Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146**
- **Windows SMB Information Disclosure Vulnerability – CVE-2017-0147**
- **Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148**

Mitigation

Schneider Electric recommends customers with supported systems check with their designated support portals first before executing the following to prevent this attack:

- Immediately apply the Microsoft patch for the MS17-010 SMB vulnerability: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx?utm_campaign=Customer%20Advisory%3A%20Ransomware%20%26%20NSA&utm_source=hs_email&utm_medium=email&utm_content=51891072&_hsenc=p2ANqtz-_NvE2mLBDpHPM291B5t32lBa1Ymb4vsbyTDxRevQ2DoPbqW-1KlECy9-gEjL1kIZ4yifVn8I1IVX64iWT7x4vND3pgP614Sp6I1naq4esvOsuOZio&_hsmi=51891072
- Immediately update your virus definitions (DAT file). McAfee has released an emergency DAT to include coverage for Ransom-WannaCry.
- We recommend keeping your virus definition files current by updating frequently. McAfee DAT files are typically updated daily and posted to our EndPoint Protection web page: https://support.ips.invensys.com/content/mcafee2/vscan2.asp by 9AM EST or as required.
- Ensure you have up-to-date backups. This alone is the most effective way to recover from a ransomware attack.
- Ensure all other cyber-defenses are up-to-date. If you are unclear then seek engagement with the cyber-services team: http://www.schneider-electric.com/b2b/en/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp
- Enable strong spam filters to prevent phishing e-mails from reaching the end users and authenticate in-bound e-mail.
- Configure access controls including file, directory, and network share permissions with least privilege in mind.
- Disable macro scripts from Microsoft Office files transmitted via e-mail.
- Inform and educate your employees to identify scams, malicious links, and social engineering attempts.

For More Information

- US-CERT Alert (TA17-132A) Indicators Associated with WannaCry Ransomware: https://www.us-cert.gov/ncas/alerts/TA17-132A
- McAfee KB89335 Protecting against Ransom-WannaCry: https://kc.mcafee.com/corporate/index?page=content&id=KB89335
- Microsoft Security Response Center article Customer Guidance for WannaCrypt attacks:https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ NOTE: this article also provides information regarding Windows XP and Windows Server 2003.

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric: Schneider Electric is the global specialist in energy management and automation. With revenues of €27 billion in FY2015, our 160,000 employees serve customers in over 100 countries, helping them to manage their energy and processes in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies will reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2017.05.15 11:44:49 -04'00'