

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

**<http://www.us-cert.gov/tlp/>**

**DATE(S) ISSUED:**

07/25/2016

**SUBJECT:**

Multiple Vulnerabilities in Siemens Products Could Allow For Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in the Siemen's SIMATIC WinCC and PCS software, which could allow for remote code execution. PCS is a distributed control system (DCS) integrating SIMATIC WinCC. SIMATIC WinCC is a SCADA system that is used to monitor and control physical processes involved in industry and infrastructure. This software is used in many industries, including food and beverage, water and wastewater, oil and gas, and chemical. Successful exploitation of these vulnerabilities could allow a remote attacker to execute code to take control of the system.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

SIMATIC PCS 7 (WinCC, Batch, Route Control, OPEN PCS 7)

- V7.1 SP4 and earlier versions
- V8.0: All versions
- V8.1: All versions
- V8.2: All versions

SIMATIC WinCC

- V7.0 SP 2 and earlier versions
- V7.0 SP 3: All versions
- V7.2: All versions
- V7.3: All versions < 7.3 Update 10
- V7.4: All versions < 7.4 Update 1

SIMATIC WinCC Runtime Professional: All versions < V13 SP 1 Update 9

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: N/A**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in SIMATIC WinCC and PCS software. Details of these vulnerabilities are as follows:

- A vulnerability found in SIMATIC WinCC or WinCC Runtime Professional could allow for unauthenticated users to remotely execute code by sending specially crafted packets. (CVE-2016-5743)
- An arbitrary file read vulnerability found in SIMATIC WinCC that could allow unauthenticated users to extract arbitrary files from a WinCC station by sending specially crafted packets.(CVE-2016-5744)

Successful exploitation of these vulnerabilities could allow a remote attacker to execute code to take control of the system.

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Siemens to vulnerable systems, as available, immediately after appropriate testing.
- Always run WinCC, WinCC Runtime Professional and PCS 7 stations within a trusted network and ensure they communicate only via trusted channels.
- Whitelist trusted networks and clients.
- Only allow trusted traffic over TCP port 1433.
- Deactivate all unnecessary users on the WinCC server.

**REFERENCES:**

**Siemens:**

[http://www.siemens.com/cert/pool/cert/siemens\\_security\\_advisory\\_ssa-378531.pdf](http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-378531.pdf)

[https://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational\\_guidelines\\_industrial\\_security\\_en.pdf](https://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf)

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5743>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5744>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

**<http://www.us-cert.gov/tlp/>**