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
https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

09/15/2021

SUBJECT:

Multiple Vulnerabilities in Siemens SIPROTEC 5 Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Siemens SIPROTECT 5, the most severe of which could allow an attacker to cause a denial-of-service condition or arbitrary code execution. Siemens SIPROTEC 5 is part of the new generation of modular, flexible, and intelligent digital field devices for protection, control, monitoring, and measuring applications in electrical energy systems. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then view or modify data, as well as take full control of the system.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- SIPROTEC 5 relays with CPU variants CP050: All versions prior to 8.80
- SIPROTEC 5 relays with CPU variants CP100: All versions prior to 8.80
- SIPROTEC 5 relays with CPU variants CP150: All versions
- SIPROTEC 5 relays with CPU variants CP200: All versions
- SIPROTEC 5 relays with CPU variants CP300: All versions prior to 8.80

RISK:

Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Siemens SIPROTEC 5, the most severe of which could allow for arbitrary code execution in the context of the system.

Details of the vulnerabilities are as follows:

- Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') - An attacker can send specially crafted packets to port 4443/TCP, which may cause a denial-of-service condition or remote code execution. (CVE-2021-33719)
- Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') - An attacker can send specially crafted packets to port 4443/TCP, which may cause a denial-of-service condition. (CVE-2021-33720)
- Improper Input Validation - Received web packets are not properly processed. An unauthenticated remote attacker with access to any of the Ethernet interfaces could send specially crafted packets to force a restart of the target device. (CVE-2021-37206)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the system. Depending on the privileges associated with the user, an attacker could then view or modify data, as well as take full control of the system.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Siemens immediately after appropriate testing.
- Verify that all hosts with a public IP do not have open ports unless absolutely necessary.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Siemens:

https://cert-portal.siemens.com/productcert/pdf/ssa-847986.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-500748.pdf

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33719
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37206

US-CERT:

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-10
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-16

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.