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:
07/15/2021

SUBJECT:
A Vulnerability in Schneider Electric Modicon PLCs Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Schneider Electric Modicon PLCs, which could result in remote code execution. A Programmable Logic Controller, or PLC, is a ruggedized computer used for industrial automation. These controllers can automate a specific process, machine function, or even an entire production line. Successful exploitation of this vulnerability could allow for remote code execution within the context of a privileged process. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are no reports of this vulnerability being exploited in the wild

SYSTEMS AFFECTED:
- Modicon M580 CPU (part numbers BMEP and BMEH), all versions
- Modicon M340 CPU (part numbers BMXP34), all versions

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

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

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Schneider Electric Modicon PLCs, which could result in remote code execution. Schneider Electric Modicon PLCs are prone to a design error security bypass vulnerability that could allow a threat actor to run arbitrary code within the context of a privileged process. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user

rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate mitigations provided by Schneider Electric as there is no available patch as this time
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-22779

HelpNet Security:
https://www.helpnetsecurity.com/2021/07/13/cve-2021-22779/

Schneider Electric:
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-194-01

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.