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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
03/14/2022

SUBJECT:
Multiple Vulnerabilities in Schneider Electric APC Smart-UPS Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Schneider Electric APC Smart-UPS that could allow for remote code execution. Schneider Electric APC Smart-UPS are devices that protect equipment and provide emergency backup power for mission-critical assets. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application. 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.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- SMT Series UPS 04.5, 09.8, 01.2, 03.1, and prior
- SMTL Series UPS 02.9 and prior
- SMC Series UPS 04.2, 14.1, 11.0, 01.1 and prior
- SCL Series UPS 02.5, 03.1 and prior
- SMX Series UPS 03.1 10.2, 07.0 and prior
- SRT Series UPS 08.3, 01.0, 10.4, 12.2, 05.1, 05.2, and prior

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 Schneider Electric APC Smart-UPS that could allow for remote code execution. Details of the vulnerabilities are as follows:

- An Improper Authentication vulnerability exists that could cause an attacker to arbitrarily change the behavior of the UPS if a key is leaked and used to upload malicious firmware. (CVE-2022-0715)
- A Buffer Copy without Checking Size of Input vulnerability exists that could cause remote code execution when an improperly handled TLS packet is reassembled. (CVE-2022-22805)
- An Authentication Bypass by Capture-replay vulnerability exists that could cause unauthenticated connection to the UPS when a malformed connection is sent. (CVE-2022-22806)

Note: To exploit CVE-2022-22805 and CVE 2022-22806, an attacker would need to conduct a Man-in-the-Middle attack which would enable them to impersonate Schneider Electric Cloud and push a maliciously crafted firmware to the targeted devices.

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application. 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:
We recommend the following actions 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=CVE-2022-0715

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22805

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22806

HelpNet Security:
https://www.helpnetsecurity.com/2022/03/08/ups-devices-vulnerabilities/

Schneider Electric:
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-067-02