ICS ADVISORY

Schneider Electric PowerLogic PM5560

Last Revised: August 28, 2018 **Alert Code:** ICSA-18-240-03

1. EXECUTIVE SUMMARY

- **CVSS v3 8.2**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Schneider Electric
- **Equipment:** PowerLogic PM5560
- **Vulnerability:** Cross-site Scripting

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow user input to be manipulated, allowing for remote code execution.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of PowerLogic PM5560, a power management system, are affected:

- PowerLogic PM5560 all versions prior to firmware Version 2.5.4

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING') CWE-79 <https://cwe.mitre.org/data/definitions/79.html>

The PowerLogic PM5560 product is susceptible to cross-site scripting attack on its web browser. An attacker may be able to manipulate inputs to cause execution of java script code.

CVE-2018-7795 has been assigned to this vulnerability. A CVSS v3 base score of 8.2 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:r/s:c/c:h/i:l/a:n>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Energy
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** France

3.4 RESEARCHER

Schneider Electric, working with Ezequiel Fernandez and Bertin Jose, reported this vulnerability to NCCIC.

4. MITIGATIONS

Schneider Electric has released a fix to address this vulnerability:

https://www.schneider-electric.com/en/download/document/PM5560_PM5563_V2.5.4_Release/
<https://www.schneider-electric.com/en/download/document/pm5560_pm5563_v2.5.4_release/>

For more information please see the Schneider Electric security notification at:

https://www.schneider-electric.com/en/download/document/SEVD-2018-228-01/
<https://www.schneider-electric.com/en/download/document/sevd-2018-228-01/>

NCCIC recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet </ics/alerts/ics-alert-10-301-01>.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

NCCIC also provides a section for control systems security recommended practices </ics/content/recommended-practices> on the ICS-CERT web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS-CERT website </ics/> in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to NCCIC for tracking and correlation against other incidents.

No known public exploits specifically target this vulnerability.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Schneider Electric

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov