Eaton Vulnerability Advisory

ETN-VA-2022-1008: Security issue in SMP Gateway automation platform

Date	Overall Risk	CVSS v3.1
07/07/2023	Medium	4.7

Overview

Eaton has been made aware of security vulnerability in the Web Server of its SMP Gateway automation platform. The platform provides data concentration, protocol translation and logic processing, a built-in HMI and secure remote maintenance access to substation and field devices, reducing operating costs and increasing productivity for a large variety of applications.

Vulnerability Details

CVE-2023-43775

CVSS v3.1 Base Score – CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

Successful exploitation of the issue can potentially lead to an unexpected restart of the SMP Gateway automation platform, impacting the availability of the product. In rare situations, the issue could cause the SMP device to restart in Safe Mode or Max Safe Mode. When in Max Safe Mode, the product is not vulnerable anymore.

In all scenarios, the remote access to the SMP device is not lost. It is possible to connect to the SMP device using the maintenance tools to apply the remediation and/or the mitigation measures (see below).

Affected Product(s) and Version(s)

Below is the list of products which are impacted by the security issue:

- **SMP SG-4260** – All 8.0 versions before 8.0R9, all 8.1 versions before 8.1R5 and all 8.2 versions before 8.2R4
- **SMP SG-4250** – All 7.0, 7.1, 7.2 versions, all 8.0 versions before 8.0R9, all 8.1 versions before 8.1R5 and all 8.2 versions before 8.2R4
- **SMP 4/DP** – All 6.3, 7.0, 7.1, 7.2 versions, all 8.0 versions before 8.0R9, all 8.1 versions before 8.1R5 and all 8.2 versions before 8.2R4
- **SMP 16** – All 6.3, 7.0, 7.1, 7.2 versions and all 8.0 versions before 8.0R9

Eaton Vulnerability Advisory

Remediation & Mitigation

Remediation

Eaton has patched the security flaw and released new versions for the affected products.

Following are the details for the affected products

- **SMP SG-4250 and SMP SG-4260** – Patched versions 8.0R9, 8.1R5 and 8.2R4
- **SMP 4/DP** – Patched versions 8.0R9, 8.1R5 and 8.2R4
- **SMP 16** – Patched versions 8.0R9

The patched versions can be obtained from here – https://gridsolutions.eaton.com/

Versions 6.3, 7.0, 7.1, 7.2, all 8.0 versions before 8.0R9, all 8.1 versions before 8.1R5 and all 8.2 versions before 8.2R4 are not patched.

Eaton highly recommends that customers and or end-users implement these patches as soon as possible.

Mitigation

Eaton recommends implementing the below mitigation measures only in the case where the users are unable to apply the above patches.

The users can leverage the SMP Gateway's firewall to significantly reduce the attack surface by allowing connections only from specific IP addresses and subnets to the Web Server.

SMP Gateway automation platform users are advised to install the SMP device on a private network or inside an ESP (Electronic Security Perimeter) or completely disable the Web Server in the configuration file to mitigate this vulnerability.

General Security Best Practices

- Restrict exposure to external network for all control system devices and/or systems and ensure that they are not directly accessible from open internet.
- Deploy control system networks and remote devices behind barrier devices (e.g., firewall), and isolate them from the business network.
- Remote access to control system network shall be made available only on need to use basis. Remote access shall use secure methods, such as Virtual Private Networks (VPNs), updated to the most current version available.
- Regularly update/patch software/applications to latest versions available, as applicable.
- Enable audit logs on all devices and applications.

- Disable/deactivate unused communication channels, TCP/UDP ports and services (e.g., SNMP) on the devices.
- Create security zones for devices with common security requirements using barrier devices (e.g., firewall).
- Use complex secure passwords.

Perform regular security assessments and risk analysis of your control systems. For more information on Security best practices refer to the following:

- Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN)
- Cybersecurity Best Practices Checklist Reminder (WP910003EN)

Acknowledgement

Eaton thanks the below researcher(s) for their coordinated support on the security vulnerabilities:

- CVE-2023-43775 – Communications Security Establishment, Canada.

Additional Support and Information

For additional information, including a list of vulnerabilities that have been reported on our products and how to address them, please visit our Cybersecurity web site www.eaton.com/cybersecurity, or contact us at PSIRT@eaton.com.

Legal Disclaimer:

About Eaton:

Eaton Vulnerability Advisory

Eaton is a power management company. We provide energy-efficient solutions that help our customers effectively manage electrical, and mechanical power more efficiently, safely, and sustainably. Eaton is dedicated to improving the quality of life and the environment through the use of power management technologies and services. Eaton has approximately 85,000 employees and sells products to customers in more than 175 countries.

Revision Control:

Date	Version	Notes
07/07/2023	v1.0	Initial Public Advisory
10/03/2023	v1.1	Updated Advisory

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com