Security Notification – MGE Network Management Card Transverse installed in MGE UPS and MGE STS

15-Mar-18

Overview

Schneider Electric has become aware of vulnerabilities in the MGE SNMP/Web Card 66074.

Vulnerability Overview

The vulnerabilities identified include:

1. Authorization Bypass
2. Information Exposure
3. Improper Authorization
4. Cleartext Transmission of Sensitive Information

Product(s) Affected

Product(s) affected:

MGE SNMP/Web Card Transverse

MGE Network Management Card Transverse, part number: SF66074. All card versions affected, when installed in following products:

- MGE Galaxy 5000
- MGE Galaxy 6000
- MGE Galaxy 9000
- MGE EPS 7000
- MGE EPS 8000
- MGE EPS 6000
- MGE Comet UPS
- MGE Galaxy PW
- MGE Galaxy 3000
- MGE Galaxy 4000

- STS (MGE Upsilon)

Vulnerability Details

The list of vulnerabilities identified are below:

1. **Authorization Bypass**
   Overall CVSS Score: **10.0 (Critical**
   (CVSS V3 Vector): **3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H**
   CVE ID: CVE-2018-7243 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7243**

The integrated web server (Port 80/443/TCP) of the affected devices could allow a remote attacker to get a full access to device, bypassing the authorization system.

2. **Information Exposure**
   Overall CVSS Score: **5.3**
   (CVSS V3 Vector): **3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N**
   CVE ID: CVE-2018-7244 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-72434**

The integrated web server (Port 80/443/TCP) of the affected devices could allow a remote attacker to obtain sensitive device information if network access was obtained.

3. **Improper Authorization**
   Overall CVSS Score: **7.3**
   (CVSS V3 Vector): **3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L**
   CVE ID: CVE-2018-7245: **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-72435**

The integrated web server (Port 80/443/TCP) of the affected devices could allow a remote attacker to change UPS control and shutdown parameters or other critical settings without authorization.

4. **Cleartext Transmission of Sensitive information**
   Overall CVSS Score: **10.0**
   (CVSS V3 Vector): **3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H**
   CVE ID: CVE-2018-7246 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-72436**

The integrated web server (Port 80/443/TCP) of the affected devices could allow remote attackers to discover an administrative account. If default on device, it is not using a SSL in settings and if multiple request of the page "Access Control" (IP-address device/ups/pas_cont.htm) account data will be sent in cleartext.

Mitigations

1. Authorization Bypass

This issue is present only for the 'Access control' page. The issue is not present on 'Notify application' and 'Networks' pages.

Mitigation:

Galaxy 5000	Replace by NMC kit G5K9635CH
MGE Galaxy 6000	Replace by NMC kit G5K9635CH
MGE Galaxy 9000	Replace by NMC kit G5K9635CH
MGE EPS 7000	Replace by NMC kit G9KEPS9635CH
MGE EPS 8000	Replace by NMC kit G9KEPS9635CH

For the following devices, there is no replacement NMC kit.

- MGE EPS 6000
- Comet UPS
- Galaxy PW
- Galaxy 3000
- Galaxy 4000
- STS - MGE Upsilon

We strongly recommend following cybersecurity best practices to reduce risk:

- Locate systems and remote devices behind firewalls and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the device, peripheral equipment or networks.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all devices and/or systems and ensure that they are not accessible from the Internet. 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.

2. Information Exposure

In the 'access control' page, a configuration change can be made to enable Authentication for all html pages. This setting can be configured by the customer at installation.

3. Improper Authorization

In the 'access control' page, a configuration change can be made to enable Authentication for all html pages. This setting can be configured by the customer at installation.

4. Cleartext Transmission of Sensitive information

This can be mitigated by selecting SSL mode as the default mode of the card.

Acknowledgements

Schneider Electric would like to thank the following for all their efforts related to identification of these vulnerabilities:

- Ilya Karpov (Positive Technologies)
  - **CVE-2018-7243**
  - **CVE-2018-7244**
  - **CVE-2018-7245**
  - **CVE-2018-7246**
- Evgeny Druzhinin (Positive Technologies)
  - **CVE-2018-7244**
- Stephen Nosov (Positive Technologies).
  - **CVE-2018-7243**

For More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *15 March 2018*	Original Release

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2018.03.28 16:45:35 -04'00'