

Eaton Vulnerability Advisory

ETN-VA-2020-1001: Arbitrary code execution through “Update Manager” Class

Publish Date	Affected Eaton Product(s) & Version(s)	CVE ID(s)	Severity
3/20/2020	Eaton UPS Companion Software v 1.05 & Prior	CVE-2020-6650	High

Overview

Eaton is aware of security vulnerability in UPS Companion software used to monitor the UPS at home to commercial environment.

Vulnerability Details

CVE-2020-6650

CVSS v3 Base Score – 8.3 High |AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE – 95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

UPS companion software v1.05 & Prior is affected by 'Eval Injection' vulnerability. The software does not neutralize or incorrectly neutralizes code syntax before using the input in a dynamic evaluation call e.g. "eval" in "Update Manager" class when software attempts to see if there are updates available. This results in arbitrary code execution on the machine where software is installed.

Remediation & Mitigation

Remediation

The vulnerability is now fixed in UPS Companion Software v1.06 and available for download below: - <http://powerquality.eaton.com/Support/Software-Drivers/Downloads/UPS-Companion.asp>

Product Description

Eaton UPS Companion provides safe system shutdown for SOHO, small business & Residential users looking for an easy way to enhance the protection capabilities of their Eaton UPS. Eaton UPS Companion allows an easy configuration procedure for shutdown parameters, and user-friendly access to UPS settings. Eaton UPS Companion also provides data on energy usage and energy cost for a better understanding of the power expense required for the protected equipment.

Eaton Vulnerability Advisory

General Security Best Practices

Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control.

Eaton recommends opening only those ports that are required for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems.

For more details on Security best practices please follow below whitepapers –

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):

http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

Acknowledgement

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

- CVE-2020-6650 – Ravjot Singh Samra

Additional Support and Information

For additional information or 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 you can contact us at CybersecurityCOE@eaton.com.

Legal Disclaimer:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. EATON, ITS AFFILIATES, SUBSIDIARIES, AND AUTHORIZED REPRESENTATIVES HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND/OR CONDITIONS OF SECURITY, COMPLETENESS, TIMELINESS, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS, SO THE ABOVE LIMITATIONS MAY NOT APPLY. TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EATON OR ITS AFFILIATES, OFFICERS, DIRECTORS, AND/OR EMPLOYEES, BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY KIND WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, ANY DIRECT,

Eaton Vulnerability Advisory

INDIRECT, INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, ACTUAL, LIQUIDATED, EXEMPLARY, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF EATON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. EATON RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND AT ITS SOLE DISCRETION.

About Eaton:

Eaton is a power management company. We provide energy-efficient solutions that help our customers effectively manage electrical, hydraulic 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 100,000 employees and sells products to customers in more than 175 countries.

Revision Control:

Date	Version	Notes
3/20/2020	v1.0	Original release of the advisory.

Office:

Eaton, 1000 Eaton Boulevard
Cleveland, OH 44122, United States
Eaton.com