Eaton Security Bulletin

ETN-SB-2020-1006: Matrix SSL security vulnerability

Date	Overall Risk	CVSS v3.0
8/4/2020	Critical	9.8

Overview

Eaton is aware of the security issues in InsideSecure MatrixSSL, a library used to provide secure communication using SSL/TLS. Users are advised to take proper actions as described in the bulletin for the affected products to ensure the security of their products.

Impacted Eaton Product(s) & Version(s)

Below are the list of products which are impacted by the security issue –

- SMP 4/DP – All 6.3, 7.0, 7.1, 7.2 versions and all 8.0 versions before 8.0R6
- SMP SG-4250 and SMP SG-4260 – All 7.0, 7.1, 7.2 versions and all 8.0 versions before 8.0R6
- SMP 16 – All 6.3, 7.0, 7.1, 7.2 versions and all 8.0 versions before 8.0R6

Note: Version 8.1R1 already includes the patch.

Vulnerability Details

CVE-2019-13470

CVSS v3 – 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-125 – Out-of-bounds Read

MatrixSSL version before 4.2.1 has an out-of-bound read during ASN.1 handling. On successful exploitation, this can potentially lead to complete compromise of the confidentiality, integrity and availability on the affected product over SSL/TLS secured communication layer.

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 4/DP – Patched versions 7.2R6 and 8.0R6
- SMP SG-4250 and SMP SG-4260 – Patched versions 7.2R6 and 8.0R6
- SMP16 – Patched versions 7.2R6 and 8.0R6

Note: Version 8.1R1 already includes the patch

The patched version can be obtained from here - https://www.cybectec.com

Eaton Security Bulletin

Mitigation

Versions 6.3, 7.0 and 7.1 are not patched.

Using the SMP Gateway's firewall, the attack surface can be significantly reduced by allowing connections only from specific IP addresses and subnets. Installing the SMP Gateway on a private network or inside an ESP (Electronic Security Perimeter) is a way of mitigating this vulnerability

General Security Best Practices

- Restrict exposure to external networks for all control system devices and/or systems and ensure that they are not directly accessible from the open Internet.
- Deploy control system networks and remote devices behind barrier devices (e.g. firewalls, data diodes) and isolate them from business networks.
- Remote access to control system networks should be made available on a strict need-to-use basis. Remote access should 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, FTP, BootP, DHCP, etc.) on networked devices.
- Create security zones for devices with common security requirements using barrier devices (e.g. firewalls, data diodes).
- Change default passwords following initial startup. Use complex secure passwords or passphrases.
- Perform regular security assessments and risk analysis of networked control systems.

For more details on cybersecurity best practices and leverage Eaton's Cybersecurity as a Service, please consult the following –

- Eaton offers a suite of cybersecurity assessment and life-cycle management services to help identify vulnerabilities and secure your operational technology network. These services can help you complete the recommended remediation and mitigation actions and strengthen your overall network security. More information about these services are available at www.eaton.com/cybersecurityservices. If you need immediate support, please call +1-800-498-2678 to connect with a representative.
- Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN)
- Cybersecurity Best Practices Checklist Reminder (WP910003EN)

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 CybersecurityCOE@eaton.com.

Legal Disclaimer:

Eaton Security Bulletin

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, 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.

Eaton Security Bulletin

Revision Control:

Date	Version	Notes
8/4/2020	v1.0	Initial release of the bulletin

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com