Notification Date: January 15, 2021

SECURITY ADVISORY

Security Vulnerabilities in Firmware Versions 5.1.3 and Older

Summary

Several critical security vulnerabilities have been discovered in Spectre RT ERT351 and B+B SmartWorx ERT351 firmware versions 5.1.3 (released in April 2015) and older. These vulnerabilities are exploitable remotely with low skills and affect any Advantech industrial cellular routers with this firmware. Most of the vulnerabilities have already been fixed in the firmware version 6.1.10 (released in July 2019), however for security reasons we strongly recommend using always the latest firmware version and configuring the routers based on the latest Security Guidelines.

Issue Description

1. **Improper Neutralization of Input During Web Page Generation (CWE-79)**

   The Web management does not neutralize special characters in the error response. It allows attackers to use a reflected XXS attack.

   Severity: Score 4.3 (Medium), CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

   Affected products: All Advantech industrial cellular routers with firmware 5.1.3 and older. The issue was fixed in version 5.2.0 (released in June 2015).

   Also known as: CVE-2019-18233

2. **Cleartext Transmission of Sensitive Information (CWE-319)**

   The Web management uses the unencrypted HTTP transmission and the Basic authentication method. The login and password are transmitted in cleartext form, which can be intercepted by attackers in the LAN. The Web management is not accessible over the (cellular) WAN by default.

   Severity: Score 9.8 (Critical), CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   Mitigation: Users should disable the HTTP and always use the HTTPS instead. The secured HTTPS transmission has been always enabled, even in the version 5.1.3.

Affected products: This affects all Advantech industrial cellular routers, which leave HTTP enabled and use it for Web management. The HTTP has been disabled by default since the version 6.2.0 (released in August 2019).

Also known as: CVE-2019-18231

3. **Improper Restriction of Excessive Authentication Attempts (CWE-307)**

   The Web management does not prevent brute-force attacks to guess the root password.

   Severity: Score 9.8 (Critical), CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   Mitigation: Since version 5.3.0 (released October 2015) the underlying Linux system reports unsuccessful login attempts through the syslog service, so users may establish a remote monitoring system to detect brute-force attack attempts.

   Affected products: All Advantech industrial cellular routers with firmware 6.1.9 and older. The brute-force attack protection has been implemented in version 6.1.10 (released in July 2019).

   Also known as: CVE-2019-18235

4. **Insufficiently Protected Credentials (CWE-522)**

   The Web management displays passwords for various services in a cleartext form, which can be spotted by an authorized person. Also, this information can be transmitted using the (unencrypted) HTTP protocol.

   Severity: Score 6.8 (Medium), CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

   Affected products: All Advantech industrial cellular routers with firmware version 6.1.4 and older. The passwords are hidden (replaced by dots) since the firmware version 6.1.5 (released January 2018).

5. **Usage of a Broken or Risky Cryptographic Algorithm (CWE-327)**

   The underlying Linux system uses an outdated DES hash algorithm (with salt) for password storage in the “/etc/passwd” file. The DES is considered insecure as cracking a DES password can nowadays take about 3 days.

   Severity: Score 7.0 (High), CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

   Affected products: All Advantech industrial cellular routers with firmware version 5.2.1 and older. A more secure MD5 hash has been used since the firmware version 5.3.0 (released in October 2015) and since the firmware version 6.2.5 (released in June 2020) the SHA256 hash is used instead.

   Also known as: CVE-2019-18237

6. **Using of vulnerable third-party software (CWE-1103)**

   The firmware version 5.1.3 (released in April 2015) uses the OpenSSL library version 1.0.1m and OpenSSH version 6.4.p1, which is affected by multiple vulnerabilities identified in mainly in 2016.

   Severity: 10.0 (Critical), CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Mitigation: Advantech monitors and continuously updates third-party software, so the latest firmware versions are free from third-party vulnerabilities. For security reasons the users are strongly recommended to use always the latest firmware version.

Affected products: All Advantech industrial cellular routers with firmware 5.2.0 and older. The firmware version 5.2.1 (released in July 2015) uses OpenSSL 1.0.1p and OpenSSH 6.8p1. The most recent firmware version 6.2.7 (released in December 2020) uses OpenSSL 1.1.1i and OpenSSH 8.0.

Also known as: CVE-2019-18239

Solution

The firmware version 6.1.10 (released in July 2019) addresses the reported vulnerabilities, except all vulnerabilities in third-party software discovered after the release date.

Older firmware versions are always affected by vulnerabilities discovered after the release date. It is therefore recommended to always use the latest firmware version. Advantech releases firmware updates at least four times each year.

Users are also recommended to review the latest Security Guidelines that provide hardening recommendations, such as a suggestion to disable the plain HTTP transport.

Acknowledgement

The vulnerabilities 1 and 2 were reported in April 2019 by Vlad Komarov from independent research group ScadaX, Evgeniy Druzhinin and Ilya Karpov of Rostelecom-Solar.

The vulnerabilities 3–6 were reported in April 2019 by Evgeniy Druzhinin and Ilya Karpov of Rostelecom-Solar.

Revision History

2021-01-15 Advisory published