December 1, 2025
RCU/Multiload II+
Firmware Vulnerability Notice

Description:

Toptech has recently discovered a critical vulnerability on some RCU II+ and Multiload II+ firmware versions.

Products affected:

Product Description:	RCU II+ and Multiload II+, PNs 4894 - 4911
Serial Number Range:	2401088 thru 2504760
Ship Dates:	March 1, 2024, thru November 24, 2025

Note: RCU II and Multiload II products are not affected.

Critical Vulnerability (High Risk/Low Probability):

With this vulnerability, someone on the local network with specific technical knowledge, could access the file system, start/stop processes and execute arbitrary code with root privileges on the RCU II+ or Multiload II+ products.

Solutions:

Customers have two options to permanently close this vulnerability on affected RCU II+ and Multiload II+ units.

1. Download and run one of the two RCU II+/Multiload II+ Vulnerability Removal Tools (VRT) posted on the www.toptech.com web site.
   Toptech developed these tools to close the vulnerability with the least impact to our customers.
   It is NOT NECESSARY to stop the bay OR break the W&M seal to run this tool.
   - TMS6v (5.x+) or TMS7: Download the TMS VRT and execute at the TMS command line as:
     rcuiip_mliip_vrt <RCU II+ or ML II+ IP Addresses…>
     OR
   - TMS6 and lower, or non-TMS: Download the Windows VRT and execute on a Windows 11 computer connected to the RCU II+ or Multiload II+'s local network as:
     rcuiip_mliip_vrt.exe <RCU II+ or ML II+ IP Addresses…>

   Either tool will display the vulnerability status both before and after the vulnerability removal, see below.

2. Download and install the latest firmware posted on the www.toptech.com web site.
   It is NECESSARY to stop the bay AND break the W&M seal to load the new firmware.
   Always backup the current ML configuration before updating firmware.
   Install one of the following firmware versions to close this vulnerability:
   - 20251125_20250523_11_36_06_5_36_06-ml2p-fwupdate-C0.swu
     (latest revision)
   - 20251124_20241025_11_36_05_5_36_05-ml2p-fwupdate-C0.swu
     (latest OIML R117 W&M approved)
   - 20251124_20240730_11_36_04_5_36_04-ml2p-fwupdate-C0.swu
     (latest InMetro W&M approved)
   - 20251124_20230605_11_36_00_5_36_00-ml2p-fwupdate-C0.swu
     (latest Canada W&M approved)

Contacts:

Contact our support department for any questions.

- US: 407-332-1774 option 2 or us-support@toptech.com
- EU: +32 (0)3 250 60 70 or eu-support@toptech.com

 12/1/2025

VRT Usage Instructions:

1. Find the IP addresses for all RCU II+ and Multiload II+ units.
   a. On TMS, it may be possible to query the running LCs (Line Controllers) to obtain the IP addresses with:
   ps -aux | grep lc
2. Download and uncompress (*gunzip rcuiip_mliip_vrt.gz*) the TMS or Windows VRT tool.
3. At a command prompt, execute the VRT specifying each IP address on the command line. For example:
   rcuiip_mliip_vrt 192.168.1.100 192.168.1.101
4. For each device, note the results of the vulnerability removal.
   Typical output from the VRT:

```
PS C:\Users\mackh> .\rcuiip_mliip_vrt.exe
Error: No operation specified.


Usage:
  rcuiip_mliip_vrt <IP/HOSTNAME>          Scan and remediate a single target
  rcuiip_mliip_vrt -i, --interactive      Launch interactive REPL mode
  rcuiip_mliip_vrt -h, --help             Show full usage


Examples:
  rcuiip_mliip_vrt 192.168.1.100
  rcuiip_mliip_vrt -i
  rcuiip_mliip_vrt --discover --subnet 192.168.1.0/24
PS C:\Users\mackh> .\rcuiip_mliip_vrt.exe 172.31.0.20 172.31.0.21 172.31.0.22

DEVICE SCAN
--------------------------------------------------------------------------------

| Target | Type | Firmware | Status |
|---|---|---|---|
| 172.31.0.20 | MultiLoad | MultiLoad II  Slate v4.36.06 May 23 2025 | Not Vulnerable |
| 172.31.0.21 | MultiLoad | RCU II  10.31.46 Dec 22 2020 | Not Vulnerable |
| 172.31.0.22 | MultiLoad | MultiLoad II+  v5.36.07 Sep 28 2025 | Vulnerable |

Scan complete: 1 vulnerable, 2 not vulnerable

The following targets are NOT vulnerable and will be skipped:
  - 172.31.0.20
  - 172.31.0.21

REMEDIATION
--------------------------------------------------------------------------------

[*] Processing target: 172.31.0.22
[OK] Remediation successful on 172.31.0.22
     Vulnerability remediated (No connection could be made because the target machine actively refused it. (os error 10061))

RESULTS
--------------------------------------------------------------------------------

| Target | Type | Initial State | Remediation | Verify |
|---|---|---|---|---|
| 172.31.0.22 | MultiLoad | Vulnerable | OK | OK |

Total: 1 result(s) - 1 succeeded, 0 failed/skipped

PS C:\Users\mackh>
```