WESTERMO-SW6-23-01: Security Advisory

CRITICAL / HIGH / MEDIUM / LOW / INFORMATIONAL 2023-01-11

Security Vulnerability SNMPv3

Description

All Ibex Software 6 releases up to and including version **6.10.1-0** have a security vulnerability on units with SNMPv3 (v3usm) enabled.

By default, SNMP is enabled with SNMPv2 (v2c). This means that unless you have actively enabled SNMPv3 you are not vulnerable.

The vulnerability means that under some circumstances an attacker can get un-authorized access via SNMP.

It is highly recommended to upgrade the unit to Software 6 release with version **6.10.1-1** or later.

Please see the MIB reference in the *Software 6 Management Guide* for more information about available configuration options.

Affected versions

All Ibex products running Software 6 versions are affected.

Severity

The CVSSv3.1 severity base score is: **9.5**

Mitigation

There are several ways to mitigate this vulnerability:

- Upgrade to Software 6 firmware release with version **6.10.1-1** or later
- Disable SNMPv3 on all interfaces (See cfgSnmpdEnabled)
- Use SNMPv2 (v2c) instead of SNMPv3 (v3usm) (See cfgSnmpdVersion). Please note that SNMPv2 does not offer any encryption.

References

- Download Ibex Software 6 - 6.10.1-1 (zip, 55MB)
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H