TECSON/GOK Improper Authentication and Access Control on multiple devices

VDE-2019-012

CVE Identifier: CVE-2019-12254
Severity: Critical 9.8 (CVSS:3.0:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Affected Vendors:
TECSON
GOK
Affected Products:
LX-Net
LX-Q-Net
e-litro net
SmartBox 4 LAN
SmartBox 4 LAN PRO

Vulnerability Type:
Improper Authentication and Access Control (CWE-287)

Summary:
A security researcher discovered that the affected application doesn't properly restrict access to an endpoint that is responsible for saving settings, to a user with limited access rights. Based on the lack of adequately implemented access-control rules, by accessing a specific uniform resource locator (URL) on the web server, a malicious user is able to change the application settings without authenticating at all, which violates originally laid ACL rules.

Impact:
This issue allows changing the configuration and get full access to the web-based configuration interface of the device wich includes all settings like passwords, alerting parameters and output states. That can adversely affect the planned operation of the equipment or can aid in further attacks on the industrial control process.

Temporary Fix / Mitigation:
In secure environments disable port forwarding and remote access to the device otherwise disable network access completely.

Solution:
Update the device to firmware V6.3.x or later as soon as it is available to fix the vulnerability.

Reported by:
Maxim Rupp (rupp.it), coordinated by CERT@VDE (cert.vde.com)

TECSON/GOK unsachgemäße Authentifizierungs- und Zugriffskontrolle bei mehreren Geräten

VDE-2019-012

CVE Identifier: CVE-2019-12254
Schweregrad: Kritisch 9.8 (CVSS:3.0:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Betroffene Hersteller:
TECSON
GOK
Betroffene Produkte:
LX-Net
LX-Q-Net
e-litro net
SmartBox 4 LAN
SmartBox 4 LAN PRO

Typ der Schwachstelle:
Unsachgemäße Authentifizierungs- und Zugriffskontrolle (CWE-287)

Zusammenfassung:
Durch einen Sicherheitsforscher wurde entdeckt, dass die betroffene Anwendung den Zugriff auf einen Endpunkt, der für das Abspeichern der Konfiguration zuständig ist, für nicht authentifizierte Benutzer nicht ordnungsgemäß verhindert. Auf der Grundlage der nicht angemessen Zugriffskontrolle kann ein Angreifer durch den Aufruf einer bestimmten URL die Konfiguration und Einstellungen verändern ohne sich überhaupt identifizieren zu müssen.

Auswirkungen:
Die Schwachstelle erlaubt vollen Zugriff und das Verändern der Web basierten Schnittstelle, welche alle Einstellungen wie Passworte, Benachrichtigungsparameter und die Zustände der Ausgänge beinhaltet. Dies kann sich schädlich für den geplanten Einsatzzweck auswirken oder weitere Angriffe auf einen Steuerungsprozess begünstigen.

Vorübergehende Schutzmaßnahmen / Schadenminderung:
Deaktivieren sie in sicheren Netzwerkumgebungen die Portweiterleitung und andere Möglichkeiten des Fernzugriffs. In anderen Fällen deaktivieren sie den Netzwerkzugriff komplett.

Lösung:
Aktualisieren sie die Firmware auf V6.3.x oder später sobald die Firmware zur Verfügung steht.

Gemeldet von:
Maxim Rupp (rupp.it), koordiniert vom CERT@VDE (cert.vde.com)