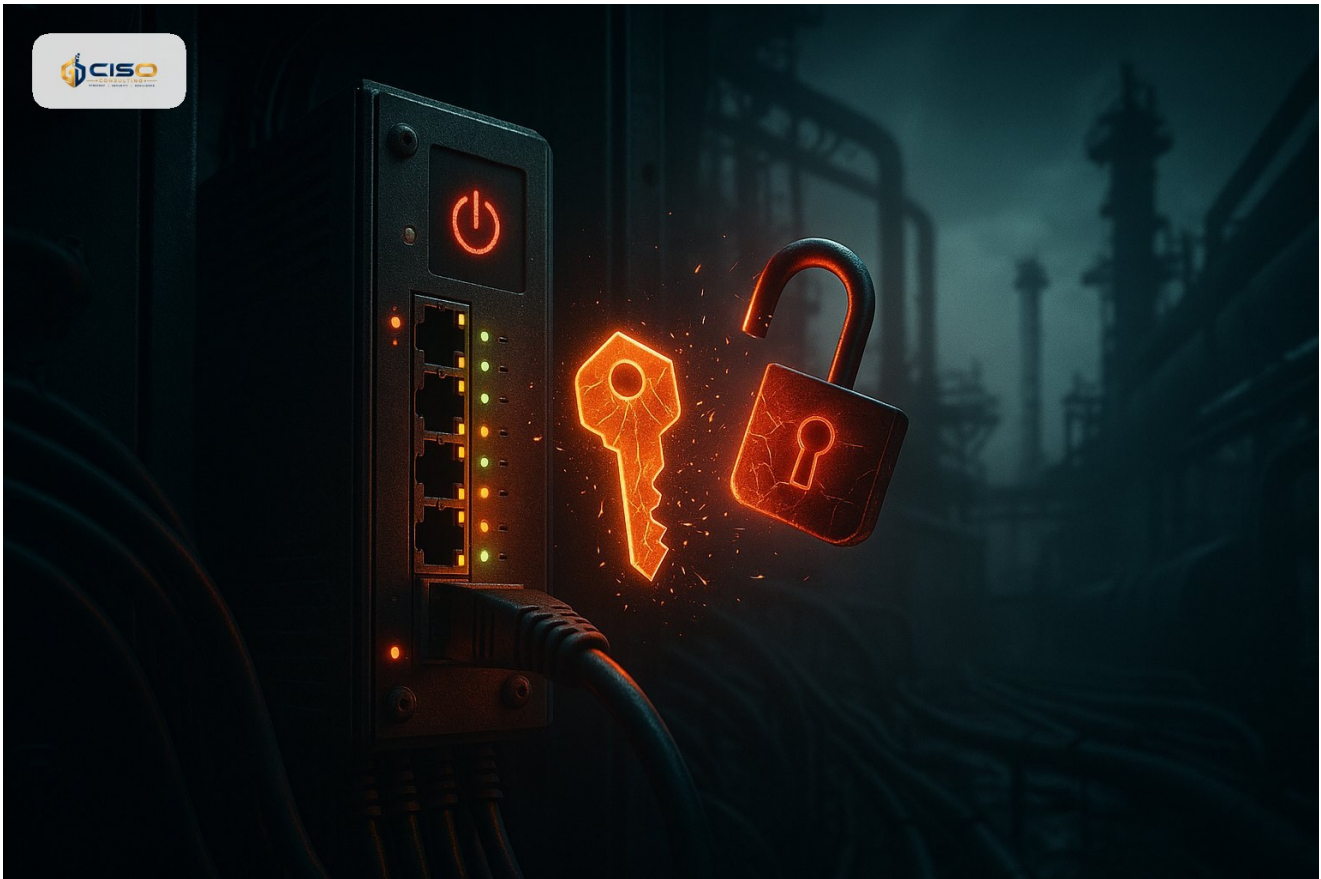


CISA warns of authentication and credential flaws in Red Lion N-Tron 700 industrial switches



CISA has published an advisory for seven vulnerabilities in Red Lion Controls N-Tron 700 Series industrial switches that could allow unauthorised administrative access and remote device reboots.

- Seven vulnerabilities affect Red Lion N-Tron 700 Series switches running firmware version 3.11.0 or earlier and bootloader 2.0.6.1 or earlier
- Flaws include hard-coded credentials, insufficiently protected credentials, missing authentication, and authentication bypass mechanisms
- Successful exploitation grants administrative access to view, edit and upload configuration files
- Attackers can force continuous device reboots by navigating to a specific URL, which can be automated via script

- CVSS score of 8.3 indicates high severity for critical infrastructure environments

The United States Cybersecurity and Infrastructure Security Agency has issued an industrial control systems advisory for multiple vulnerabilities affecting Red Lion Controls N-Tron 700 Series managed industrial Ethernet switches. The flaws carry a combined CVSS score of 8.3 and affect devices running firmware version 3.11.0 or earlier and bootloader version 2.0.6.1 or earlier.

Vulnerability profile

The advisory identifies seven distinct CVE entries spanning authentication and credential management weaknesses. The vulnerabilities include **hard-coded credentials**, insufficiently protected credentials, passwords stored in recoverable format, missing authentication for critical functions, code download without integrity checks, reachable assertion flaws, and authentication bypass through alternate paths. Successful exploitation enables a malicious actor to gain full administrative access to the device, permitting viewing, editing and uploading of configuration files.

Denial-of-service risk

Beyond unauthorised access, the vulnerabilities allow an attacker to trigger device reboots by navigating to a specific URL on the switch. This action can be scripted and automated on an attacker's local machine to cause continuous rebooting, effectively creating a **denial-of-service condition** that disrupts network operations in industrial environments.

Implications for regulated environments

For organisations operating critical infrastructure or industrial control systems in Saudi Arabia, these vulnerabilities present operational continuity and integrity risks. The affected switches are commonly deployed in manufacturing, utilities and other operational technology environments where network availability and configuration integrity are essential to safety and compliance obligations.

What to do now

1. Identify all Red Lion N-Tron 700 Series switches in operational technology and industrial control networks across your organisation
2. Check firmware and bootloader versions on identified devices; prioritise those running firmware 3.11.0 or earlier and bootloader 2.0.6.1 or earlier
3. Contact Red Lion Controls or your authorised distributor for patch availability and upgrade guidance
4. Implement network segmentation to isolate affected switches from untrusted networks and restrict administrative access to authorised personnel only
5. Monitor device logs and network traffic for unusual administrative access attempts or repeated reboot

events

6. Review and update incident response procedures to address potential denial-of-service scenarios affecting industrial network infrastructure