مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in MICROSENS NMP

Tracking #:432317437

Date:02-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities have been discovered in MICROSENS NMP Web+, a widely deployed industrial network management platform.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been discovered in MICROSENS NMP Web+, a widely deployed industrial network management platform. These flaws can allow unauthenticated remote attackers to gain full control over the affected systems with low complexity and no user interaction.

The impacted software is extensively used in critical infrastructure, particularly in manufacturing and industrial automation, significantly increasing the risk of large-scale operational disruption or nation-state cyberattacks.

Vulnerability Details:

CVE ID	Vulnerability Name	CVSS v3	CVSS v4	Description
CVE-2025-49151	Use of Hard-coded, Security-relevant Constants	9.1	9.3	A hardcoded JWT secret key allows attackers to forge valid tokens, enabling unauthenticated access to sensitive components.
CVE-2025-49152	Insufficient Session Expiration	7.5	8.7	Expired JWTs remain valid, allowing attackers to retain persistent access after token compromise.
CVE-2025-49153	Improper Limitation of a Pathname to a Restricted Directory	9.8	9.3	A path traversal flaw enables attackers to overwrite system files and execute arbitrary code with remote access.

These vulnerabilities may be chained together to escalate access and fully compromise the affected system remotely without user interaction

Fixed Versions:

- MICROSENS NMP Web+ v3.3.0 on both Windows and Linux

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update MICROSENS NMP Web to fixed version for both Windows and Linux platforms to patch all vulnerabilities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.microsens.com/support/downloads/nmp/