

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in Eaton UPS Companion (EUC) Software

Tracking #:432318207

Date:05-01-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Eaton UPS Companion (EUC) software that could be exploited to allow arbitrary code execution on the host system, potentially compromising systems used to monitor and manage critical power infrastructure.

TECHNICAL DETAILS:

Vulnerability Details

CVE-2025-59887 – Insecure Library Loading (DLL Hijacking)

- **CVSS Score:** 8.6 (High)
- The EUC software installer is vulnerable to insecure library loading. An attacker with access to the installation directory could place a malicious library that is loaded instead of a legitimate system library during installation, resulting in arbitrary code execution with the privileges of the installing user.

CVE-2025-59888 – Unquoted Search Path Vulnerability

- **CVSS Score:** 6.7 (Medium)
- Due to improper quotation of search paths within the Eaton UPS Companion software, an attacker with file system access could exploit the vulnerability to execute arbitrary code on the host system.

Impact

Exploitation of these vulnerabilities could result in system compromise, unauthorized code execution, and potential disruption of power monitoring operations.

Affected Versions

- Eaton UPS Companion (EUC) versions prior to 3.0

Fixed Version

- Eaton UPS Companion (EUC) version 3.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Eaton UPS.

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://nvd.nist.gov/vuln/detail/CVE-2025-59887>
- <https://nvd.nist.gov/vuln/detail/CVE-2025-59888>