



NCSC-2025-0221

Kwetsbaarheden verholpen in Schneider Electric EcoStructure IT Datacenter Expert

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-07-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Schneider Electric heeft kwetsbaarheden verholpen in EcoStructure IT Datacenter Expert.

Duiding

De kwetsbaarheden omvatten onder andere onvoldoende controle over speciale elementen in OS-commando's, wat kan leiden tot ongeauthenticeerde externe code-executie. Daarnaast is er een probleem met onvoldoende entropie in wachtwoordgeneratie-algoritmen, wat kan resulteren in het ontdekken van rootwachtwoorden. Verder is er een kwetsbaarheid gerelateerd aan onjuiste controle van codegeneratie, wat kan leiden tot externe opdrachtuitvoering via hostname-invoer. Ook is er een Server-Side Request Forgery (SSRF) kwetsbaarheid die ongeauthenticeerde externe code-executie mogelijk maakt door manipulatie van verborgen URL's. Bovendien is er een probleem met onjuiste privilegebeheer, wat kan leiden tot privilege-escalatie. Tot slot kan er ongeautoriseerde bestandstoegang plaatsvinden door het misbruiken van SOAP API-aanroepen en XML externe entiteiten injectie.

Oplossingen

Schneider Electric heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-189-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=sevd-2025-189-01.pdf

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-50121	10.0 CRITICAL
➤ CVE-2025-50122	8.3 HIGH
➤ CVE-2025-50123	7.2 HIGH
➤ CVE-2025-50125	7.2 HIGH
➤ CVE-2025-50124	6.9 MEDIUM

[> CVE-2025-6438](#)

6.8 MEDIUM

CWE's

CWE	Beschrijving
> CWE-331	Insufficient Entropy
> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-918	Server-Side Request Forgery (SSRF)
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-611	Improper Restriction of XML External Entity Reference
> CWE-269	Improper Privilege Management

Getroffen producten

Schneider Electric
EcoStruxure™ IT Data Center Expert

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.