Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0221

Kwetsbaarheden verholpen in Schneider Electric EcoStruxture 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 EcoStruxture 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