Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0177

Kwetsbaarheden verholpen in ABB ASPECT-productlijn

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-05-2025

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

ABB heeft kwetsbaarheden verholpen in de ASPECT-productlijn, inclusief ASPECT-Enterprise, NEXUS Series en MATRIX Series tot versie 3.08.03.

Duiding

De kwetsbaarheden omvatten onder andere Remote Code Execution, SQL-injectie, servlet-injectie, en verschillende vormen van bestandstoegang en -manipulatie. Deze kwetsbaarheden kunnen worden geëxploiteerd wanneer sessie-administratorcredentials zijn gecompromitteerd, wat kan leiden tot ongeautoriseerde toegang, controle over systemen, en ernstige gevolgen voor de integriteit en vertrouwelijkheid van gegevens. Aanvallers kunnen bijvoorbeeld willekeurige code uitvoeren, systeembronnen uitputten, gevoelige bestanden benaderen of zelfs systeembestanden verwijderen, wat kan resulteren in operationele verstoringen.

Oplossingen

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

Referenties

› https://search.abb.com/library/Download.aspx?DocumentID=9AKK108471A0021&LanguageCode=en&DocumentPartId=pdf&Action=Launch

Kwetsbaarheden

CVE	CVSS Score
› CVE-2024-9639	7.5 HIGH
› CVE-2024-13928	7.5 HIGH
› CVE-2024-13929	7.5 HIGH
› CVE-2024-13930	5.9 MEDIUM
› CVE-2024-13931	7.5 HIGH
› CVE-2024-48850	7.5 HIGH

CVE-2024-48853	9.5 CRITICAL
CVE-2025-2409	8.9 HIGH
CVE-2025-2410	8.9 HIGH
CVE-2025-30169	6.0 MEDIUM
CVE-2025-30170	5.9 MEDIUM
CVE-2025-30171	7.3 HIGH
CVE-2025-30172	8.9 HIGH
CVE-2025-30173	6.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-606	Unchecked Input for Loop Condition
CWE-286	Incorrect User Management
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-36	Absolute Path Traversal
CWE-99	Improper Control of Resource Identifiers ('Resource Injection')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-863	Incorrect Authorization
CWE-73	External Control of File Name or Path

Getroffen producten

ABB
ASPECT- Enterprise
MATRIX Series
NEXUS Series

Disclaimer