Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0465

Kwetsbaarheden verholpen in ABB ASPECT, NEXUS Series en MATRIX Series

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 06-12-2024

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 ABB ASPECT, NEXUS Series en MATRIX Series (Specifiek voor versies tot 3.08.02).

Duiding

De kwetsbaarheden omvatten ongeautoriseerde toegang tot bestanden op de webserver, wat kan leiden tot datalekken of ongeautoriseerde gegevensmanipulatie. Daarnaast zijn er ernstige kwetsbaarheden gerapporteerd met betrekking tot remote code inclusion en Cross-Site Scripting, die aanvallers in staat stellen om willekeurige code op afstand uit te voeren en kwaadaardige scripts in clientbrowsers te injecteren. Ook zijn er Server-Side Request Forgery kwetsbaarheden vastgesteld die kunnen leiden tot ongeautoriseerde toegang en mogelijke informatieonthulling. De blootstelling van gebruikersnamen en wachtwoorden in platte tekst of Base64-encoding verhoogt het risico op ongewenste credential-lekken. Bovendien zijn er Denial of Service kwetsbaarheden die de operationele continuïteit van organisaties kunnen verstoren.

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=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch

Kwetsbaarheden

CVE	CVSS Score
› CVE-2024-6209	10.0 CRITICAL
› CVE-2024-6298	10.0 CRITICAL
› CVE-2024-6515	9.6 CRITICAL
› CVE-2024-6516	9.0 CRITICAL
› CVE-2024-6784	9.9 CRITICAL

CVE-2024-11316	7.5 HIGH
CVE-2024-11317	10.0 CRITICAL
CVE-2024-48839	10.0 CRITICAL
CVE-2024-48840	10.0 CRITICAL
CVE-2024-48843	7.7 HIGH
CVE-2024-48844	7.7 HIGH
CVE-2024-48845	9.4 CRITICAL
CVE-2024-48846	7.1 HIGH
CVE-2024-48847	8.2 HIGH
CVE-2024-51541	8.2 HIGH
CVE-2024-51542	8.2 HIGH
CVE-2024-51543	8.2 HIGH
CVE-2024-51544	8.2 HIGH
CVE-2024-51545	10.0 CRITICAL
CVE-2024-51546	7.5 HIGH
CVE-2024-51548	9.9 CRITICAL
CVE-2024-51549	10.0 CRITICAL
CVE-2024-51550	10.0 CRITICAL
CVE-2024-51551	10.0 CRITICAL
CVE-2024-51554	9.1 CRITICAL
CVE-2024-51555	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')
CWE-1393	Use of Default Password
CWE-328	Use of Weak Hash
CWE-1287	Improper Validation of Specified Type of Input
CWE-522	Insufficiently Protected Credentials
CWE-15	External Control of System or Configuration Setting
CWE-193	Off-by-one Error
CWE-36	Absolute Path Traversal
CWE-319	Cleartext Transmission of Sensitive Information
CWE-521	Weak Password Requirements
CWE-552	Files or Directories Accessible to External Parties
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-918	Server-Side Request Forgery (SSRF)
CWE-384	Session Fixation
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

abb
aspect_enterprise

matrix_series
nexus_series
aspect- ent-12_firmware
aspect- ent-256_firmware

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.