NB 系列支援工具 NB-Designer

存在對 XML 外部實體引用的不當限制漏洞

發布日期: 2025 年 1 月 14 日
台灣歐姆龍股份有限公司

■ 概述

NB 系列支援工具之 NB-Designer 存在對 XML 外部實體引用的不當限制（CWE-611）漏洞。攻擊者可利用該漏洞從使用者的電腦中竊取資訊。

以下列出受此漏洞影響的產品、版本以及減輕風險的對策與迴避方法。透過執行我們建議的對策與迴避方法，可以將此漏洞被利用的風險降至最低。此外，為了讓客戶更加安心地使用產品，我們已準備了針對本次安全性強化的對策版本。關於各產品的對應版本，請參考本文中的對策方法，並請配合實施相關對策。

■ 受影響產品

受影響產品型號及其版本如下所示。

機械自動化化控制器 NJ 系列

型號	適用版本
NB-Designer	Ver.1.63 以前

如何查看受影響的版本，請參閱以下操作手冊中。

・Programmable Terminals NB-Designer Operation Manual (V106)

■ 說明

由於 NX-Designer 中存在名為「XML 外部實體引用限制不當」（CWE-611）的漏洞，攻擊者可能有機會洩露電腦上的機密資料。

■ CVSS 評分

XML 外部實體引用的不當限制漏洞（CWE-611）

CVE-2024-12298

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N 基本值 5.5

■ 對策

可以透過將產品更新到對策版本來解決此漏洞。

各產品的對策版本及其發佈時間如下所示。

可程式化人機介面 NB 系列支援工具 NB-Designer

型號	對策版本	對策版本提供時間
NB-Designer	Ver.1.64 以上	2024 年 12 月 16 日

上述對策版本的獲取途徑及更新方法，請諮詢本公司營業窗口。

■ 缓解措施和保護方法

為了將這些風險降至最低，歐姆龍建議客戶採取下列緩解措施。

1. 防毒保護

為保護任何可以存取控制系統的 PC 免受惡意軟體的侵害，請確保安裝和維護最新的商業級防毒軟體。

2. 採取安全措施，防止未授權存取

- 盡量減少控制系統和設備連接開放網路，以防不信任裝置登入。
- 使用防火墻（關閉未使用的通訊埠，限制通訊主機），將其與 IT 網路隔離。
- 使用虛擬專用網路（VPN）進行遠端連接控制系統及設備。
- 使用高強度密码並增加修改頻率。
- 安裝實物控制，确保僅授權人员可連結控制系統和設備。
- 在將任何 USB 隨身碟或類似裝置連接到系統和裝置之前，請先掃描病毒以確保其安全。
- 強化對遠端連接控制系統和設備的多重身分驗證。

3. 資料輸入和輸出保護

利用備份和範圍檢查等驗證處理措施，以防控制系統和設備輸入/輸出數據被修改。

4. 資料復原

定期進行數據備份和維護，以防數據丟失。

■諮詢方式

如您在採取減輕措施/解決方案時遇到問題，可以透過以下方式聯繫歐姆龍營業據點或經銷商：
https://www.ia.omron.com/global_network/index.html

■致謝

此漏洞由 Michael Heinzl 透過 JPCERT/CC 報告。
我們感謝 Michael Heinzl 發現並回報此漏洞。

■更新紀錄

2025 年 1 月 14 日 最新版本