Product Security Advisory

March 10, 2020

JCI-PSA-2020-3 v1
CVE-2020-9044

Overview

Johnson Controls has learned of a vulnerability impacting the *Metasys* Server software products and some network engines. The Microsoft .NET Framework low-level parser uses unsafe default parameters that makes *Metasys* software vulnerable to an XML External Entity Injection (XXE) attack.

Impact

An attacker could exploit the vulnerability to accomplish a Denial of Service attack or harvest ASCII files from the *Metasys* server.

Affected Versions

Servers and Tools	Supported Releases Affected	Unsupported Releases Affected
Application and Data Server (ADS, ADS-Lite)	9.0, 10.0, 10.1	8.1 or earlier
Extended Application and Data Server (ADX)	9.0, 10.0, 10.1	8.1 or earlier
Open Data Server (ODS)	9.0, 10.0, 10.1	8.1 or earlier
Open Application Server (OAS)	10.1	Not Applicable
System Configuration Tool (SCT)	12.0, 13.0, 13.2	11.0 or earlier

Network Engines	Supported Releases Affected	Unsupported Releases Affected
Network Automation Engine (NAE55) Network Integration Engine (NIE55/NIE59)	9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6 (not 9.0.7 or 9.0.8)	8.1
Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed)	8.1	Not Applicable
NAE85 and NIE85	9.0, 10.0, 10.1	8.1 or earlier
LonWorks® Control Server (LCS)	9.0, 10.0, 10.1	8.1 or earlier

Mitigation

Johnson Controls has developed a patch to address this issue. Contact your local branch office for remediation.

Initial Publication Date

March 10, 2020

Last Published Date

March 10, 2020

Resources

Please visit the Cyber Solutions Website https://www.johnsoncontrols.com/cyber-solutions/security-advisories to access security advisories.

Find out more about CVE-2020-9044 from NIST National Vulnerability Database (NVD) and MITRE CVE® List.