Product Security Advisory

June 4, 2021

JCI-PSA-2021-05
CVE-2021-27657
ICSA-21-159-01

Overview

Johnson Controls has confirmed a web services vulnerability impacting Metasys Servers, Engines, and SCT Tools.

Impact

Successful exploitation of this vulnerability could give an authenticated Metasys user an unintended level of access to the server file system, allowing them to access or modify system files by sending specifically crafted web messages to the Metasys system.

Note: Only an authenticated user can exploit this vulnerability. An authenticated user is someone who has access to Metasys web services via a password protected Metasys Local User Account or a Metasys Active Directory User Account.
This vulnerability was found by an independent third-party security researcher and there have been no reports of any customers affected by this issue at the publishing time of this document.

Table 1: Suggested paths of resolution for affected releases

Metasys Release	Affected	Risk level	Patch or upgrade?	Risk After Patching	Additional recommended mitigation steps
Pre-9.0	Yes	High	Upgrade to supported release1[1]	N/A	• Review all user accounts that are active or dormant and determine if they are still required through the Dormant User feature. • Delete any user accounts if the user is no longer with the company or has been promoted to another position where they no longer need to use Metasys. • Monitor the audit logs as well as the Cyber Health Dashboard, if the site has a Metasys Server at Release 10.1 or later, to monitor user activity. • Enforce a password change across the Metasys site on a regular basis.
9.0 (engine only), 10.0, 10.1, 11.0	Yes	High	Install patch	Medium	

[1] This is true for all the items except for Metasys Release 8.1 UL/cUL 864 UUKL 10th Edition Smoke Control.

Current, unpatched risk:
CVSS v3: 8.8 (high)

The patch reduces the score to:
CVSS v3: 6.3 (medium)

Note: The vulnerability will be further addressed in Metasys Release 12.0, at which point the risk level will be reduced to Low. In the meantime, the patches reduce the risk considerably.

Contact your local branch office for assistance with applying any of the solutions.

The latest release is recommended as the base version. Under typical circumstances, Johnson Controls supports the current software release and the previous major software release. For more information, refer to Metasys Software Security and Support.

It is always recommended to apply guidance from the Metasys Network and IT Guide.

The following table provides more details about the affected Metasys system product releases:

Table 2: Affected system product releases

Product	Affected releases
Application and Data Server (ADS) ADS-Lite, both Europe and Asia models Extended Application and Data Server (ADX) Metasys Energy Essentials Metasys for Validated Environments (MVE) NAE85 series network automation engine LCS85 series LonWorks Control Server Open Application Server (OAS)	All releases and patches up to and including Release 11.0
Open Data Server (ODS)	All releases and patches up to and including 10.1.2
NAE55 and NIE59 series network automation engines	All releases and patches up to and including Release 11.0
NxE25, NxE35, NxE45, NxE45-lite NIE29, NIE39, and NIE49	9.0.6 and earlier (Windows® CE) 9.0.7 and later (Linux®)
SNC and SNE engine models	All releases and patches up to and including Release 11.0
System Configuration Tool (SCT)	All releases and patches up to and including SCT 14.1
Metasys UL/cUL 864 UUKL 10th Edition	8.1 and earlier

Note: Any product that is not listed in Table 2 is not known to be impacted by this issue.

Solution

All newer patches and Metasys releases will contain this security vulnerability fix. If available and appropriate, utilize the newest patch. Otherwise, apply the appropriate patch to your Metasys product, as indicated in Table 3, Table 4, and Table 5.

Table 3: Solution for ADS, ADX, OAS, ODS, LCS85, and NAE85 by Metasys Release

Metasys Release	Solution for ADS/ADX/OAS/ODS/LCS85/NAE85
Release 9.0 and earlier	No patch available. Upgrade to a newer Metasys Release. You can directly upgrade the system from 9.0 to 10.1.3 or 11.0.1.
Release 10.0	Apply the 10.1.3 patch. You can directly upgrade the system from 10.0 to 10.1.3 or you can uninstall 10.0 first and then install 10.1.3.
Release 10.1	Apply the 10.1.3 patch. Uninstall 10.1 first and then install 10.1.3.
Release 11.0	Apply the 11.0.1 patch. Uninstall 11.0 first and then install 11.0.1.

Table 4: Solution for Network Engines by model and Metasys Release

Engine model	Solution
MS-NCE251x-0x MS-NCE251x-700 MS-NIE291x-0x MS-NCE2500-0 (Europe only) MS-NCE2506-0 (Europe only)	**Release 9.0.6 and earlier:** Apply the 9.0.9 patch using SCT Pro's Reflash feature or with the NAE Update Tool using the PXE process. **Note:** If you apply the patch to an engine at 9.0.6 and earlier, you would move from a release that has an operating system based on Windows CE to a release that is using a Linux-based operating system. **Release 9.0.7 and later:** Apply the 9.0.9 patch using SCT Pro's Reflash feature or with the NAE Update Tool using the PXE process.
MS-NCE252x-0x MS-NCE252x-700 MS-NAE352x-2x MS-NAE352x-702 MS-NAE452x-2x MS-NAE452x-702 MS-NCM452x-2x MS-NCM452x-702	No patch is available for these engines with the LonWorks Interface. If you are concerned about this vulnerability, we strongly suggest that you upgrade the hardware to a platform that supports this patch.
MS-NAE35xx-1 MS-NAE35xx-701 MS-NAE45xx-1 MS-NAE45xx-701	No patch is available. If you are concerned about this vulnerability, we strongly suggest that you upgrade the hardware to a platform that supports this patch.
MS-NAE351x-2x MS-NAE351x-702 MS-NIE391x-2x MS-NAE451x-2x MS-NAE451x-702	**Release 9.0.6 and earlier:** Apply the 9.0.9 patch using SCT Pro's Reflash feature or with the NAE Update Tool using the PXE process. **Note:** If you apply the patch to an engine at 9.0.6 and earlier, you would move from a release that has an operating system based on Windows CE to a release that is using a Linux-based operating system.

Engine model	Solution
MS-NIE491x-2x MS-NCM451x-2x MS-NCM451x-702	**Release 9.0.7 and later:** Apply the 9.0.9 patch using SCT Pro's Reflash feature or with the NAE Update Tool using the PXE process.
MS-NAE55xx-0 MS-NAE55xx-700	No patch is available. If you are concerned about this vulnerability, we strongly suggest that you upgrade the hardware to a platform that supports this patch. **Note:** Any model of engine actively using a Modem, N2 Tunneling, an N1 integration, or a WRS system will not have this functionality in Linux.
MS-NAE55xx-1 MS-NAE55xx-701	
MS-NAE55xx-2 MS-NAE55xx-702 MS-NIE59xx-2	Apply the 10.1.3 patch or the 11.0.1 patch using SCT Pro's Upgrade feature or with the NAE Update Tool using the PXE process. **Note:** Any model of engine actively using a Modem, N2 Tunneling, an N1 integration, or a WRS system will not have this functionality in Linux.
MS-NAE55xx-3 MS-NAE55xx-703 MS-NIE59xx-3	
MS-NAE5510-0U	For information about UL864 solutions, see Table 5.
MS-NAE5510-1U	
MS-NAE5510-2U	
MS-NAE5510-3U	
MS-NAE4510-2U	
MS-NAE3510-2U	
MS-NCE2560-0U	
M4-SNE10500-0	**Site Director at Release 10.1.x:** Apply the 10.1.3 patch using SCT Pro's Upgrade feature. **Site Director at Release 11.0.x:** Apply the 11.0.1 patch using SCT Pro's Upgrade feature.
M4-SNE11000-0	
M4-SNE22000-0	
M4-SNE110L0-0	
M4-SNC16120-0	
M4-SNC16120-04	
M4-SNC25150-0	
M4-SNC25150-04	
M4-SNE10501-0	
M4-SNE11001-0	
M4-SNE22001-0	
M4-SNE110L1-0	
M4-SNC16121-0	

Engine model	Solution
M4-SNC16121-0H	
M4-SNC16121-04	
M4-SNC16121-04H	
M4-SNC25151-0	
M4-SNC25151-0H	
M4-SNC25151-04	
M4-SNC25151-04H	

Table 5: Solution for UL864 Smoke Control systems by Metasys Release

Metasys Release	Solution for UL864 Smoke Control systems
Release 8.1 or earlier	There is no patch available for Smoke Control sites; these sites should follow the additional recommended mitigation steps (as outlined in Table 1, see "Additional recommended mitigation steps"). Johnson Controls is actively working on getting Metasys Release 11.0 UL/cUL 864 UUKL 10th Edition Smoke Control listed.

Initial Publication Date
June 4, 2021

Last Published Date
June 4, 2021

Resources
Cyber Solutions Website – https://www.johnsoncontrols.com/cyber-solutions/security-advisories
CVE-2021-27657 – MITRE CVE® List
ICSA-21-159-01 – CISA ICS-CERT Advisories