Security Advisory for the KUKA V/KSS WorkVisual Service Host access control vulnerability (CVE-2022-2242)

Vulnerability Name:	KUKA V/KSS WorkVisual Service Host access control vulnerability
CVE-ID:	CVE-2022-2242
Date:	2022-08-04
Severity:	critical (CVSS rating 9.8)
Vulnerability Type:	Missing Authentication for Critical Function (CWE-306)
CVSSv3 vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

The KUKA SystemSoftware V/KSS robot control systems of KUKA KR C4 and KR C5 product lines are affected by a severe access control vulnerability in the WorkVisual Service Host interface.

The KUKA SystemSoftware V/KSS versions before version 8.6.5 did not offer access control options for this interface. Solutions have been provided to fix this vulnerability for versions 8.3 to 8.6.5 (see table below for version specific details).

The KUKA SystemSoftware V/KSS introduced access control options for this interface starting with version 8.6.5. However, these options were not enabled by default, as documented in the product manual.

We recommend customers to evaluate their security requirements for existing installations to decide whether they need to restrict access to the WorkVisual Service Host interface. The default behavior will change for upcoming releases which will restrict the access by default.

Additional information

The WorkVisual Service Host interface was introduced starting with KUKA SystemSoftware V/KSS version 8.2. When access control is not available or not enabled, reading the robot configuration as well as changing the configuration are possible without any authentication and solely based on the network level access to TCP Port 49003.

Affected KUKA products

Product	Affected Version	Solution
KUKA SystemSoftware V/KSS	8.2 (KR C4)	Network isolation (see “mitigation” below) is required, and we recommend upgrading to recent versions. *Note: The product has been discontinued in 2016.*
KUKA SystemSoftware V/KSS	8.3 (KR C4)	Access control can be added with provided TechPackage for version KSS 8.3.43 HF1 and VSS 8.3.25 HF1*. *Note: The product has been discontinued in 2019.*
KUKA SystemSoftware V/KSS	8.4 (KR C4)	Network isolation (see “mitigation” below) is required. *Note: Isolation is required by the solution this product will be integrated in.*
KUKA SystemSoftware V/KSS	8.5 (KR C4)	Access control can be added with provided TechPackage for version 8.5.9 HF1*. *Note: The product has been discontinued in 2020.*
KUKA SystemSoftware V/KSS	8.6 prior to 8.6.5 (KR C4)	Upgrade to version 8.6.5 or later. Access control can then be configured (see product manual).
KUKA SystemSoftware V/KSS	8.6.5 and later (KR C4)	Access control can be configured (see product manual). Default behavior will change starting with version 8.6.10.
KUKA SystemSoftware V/KSS	8.7.0 and later (KR C5)	Access control can be configured (see product manual). Default behavior will change starting with version 8.7.5.

**) Older versions must be upgraded to the latest versions to apply the TechPackage, otherwise network isolation (see “mitigation” below) is required.*

This information reflects our current state of knowledge. We will update this statement should there be any additional information become available or in case the situation would otherwise change.

Solution

Access Control Prerequisites

1. Once the access control has been enabled, access from WorkVisual will require authentication with valid credentials for the KukaUser for read / write access (depending on the configuration).
2. WorkVisual version: WorkVisual version 6.0.5 or later are required.
3. Correct time setting: The clock of both the controller as well as the Workstation running WorkVisual must be synchronized. In case of a time deviation of more than 5 minutes, the access control feature will deny access. Please ensure the time is in sync.

A) Solution for KUKA SystemSoftware V/KSS versions from 8.6.5 onwards

With versions 8.6.5 and later the remote access restriction can be configured using the settings under “Secure remote access”, which are documented in the system software Operating and Programming Instructions (see chapter 5.6 “Restricting remote access to the robot controller” the “KSS 8.7 SI V5” manual at https://xpert.kuka.com/ID/PB14656).

B) Solution for KUKA SystemSoftware V/KSS versions from 8.6.0 to 8.6.4

For KUKA SystemSoftware V/KSS version 8.6.0 but prior to 8.6.5, an upgrade to version 8.6.5 or later is required. The upgrade can be obtained via the Customer Support.

C) Solution for KUKA SystemSoftware V/KSS versions from 8.3 to 8.5

The TechPackage *KUKA.SecuredServiceHost_1.0.0.18* has been provided to add access control for the WorkVisual Service Host interface for the latest releases of the KUKA SystemSoftware V/KSS from 8.3 to 8.5. The TechPackage can be downloaded from the Security Updates section on the KUKA homepage: https://www.kuka.com/security-updates. Once the TechPackage is installed, read and write access via WorkVisual will be restricted and will require authentication with KukaUser credentials. The TechPackage documentation includes details about additional configuration options.

Important

It is important to also change the default credentials for all Windows and smartHMI users as documented in the product manuals for end-users and system integrators (see chapter 4.14 in the “KSS 8.7 END V5” manual at https://xpert.kuka.com/ID/PB14657 and chapters 5.3 - 5.5 in the “KSS 8.7 SI V5” manual at https://xpert.kuka.com/ID/PB14656).

Info about changes in the default behavior for upcoming releases

Upcoming releases of KUKA SystemSoftware V/KSS 8.6 and 8.7 restrict the access to the WorkVisual Service Host interface by default. The setting is configurable via the smartHMI.

Workarounds and Mitigations

As a workaround for cases where the access control feature cannot be added or enabled, we recommend:

- **Restricting incoming network access** to the product altogether and only allow required traffic. In particular, traffic to TCP port 49003 should be blocked. *Note: If access to TCP port 49003 is blocked, the following services cannot be used anymore: WorkVisual, BackupManager.*
- It is still recommended to **change all Windows and smartHMI users' passwords** as documented in the product manuals (see above).

Recommended Actions

1. Review the provided solutions and follow the recommendations for your specific version(s).
2. Change the default credentials on all systems for all Windows and smartHMI users (see section "Important" above).
3. Apply the latest Security Updates https://www.kuka.com/security-updates
4. Enable access control on all systems or otherwise isolate the systems.

General Security Recommendations

In general, we recommend performing a risk assessment and based on this, to derive general protective measures for production environments (network segmentation and in particular restriction of incoming and outgoing network connections, and restriction of physical access to systems).

References

KUKA Security Updates: https://www.kuka.com/security-updates
KUKA on Cybersecurity: https://www.kuka.com/cybersecurity

Support and contact information

Customers may use their existing channels to contact the KUKA Customer Support. For all other cases, the KUKA Customer Support is available at customerservice@kuka.com

Revision history

Date	Changes
2022-08-09	Added more specific versions numbers and TechPackage name.
2022-08-04	Initial version.