



Important information regarding Heap buffer overflow from CVE-2023-5217 and CVE-2023-5129

06 October 2023



Contents

Initial response - 06.10.2023 CVE-2023-5217 and CVE-2023-5129	3
1.1 Affected products: tts performance suite since 2021r2 (producer and QuickAccess / Creator)	3
1.2 Description	3
1.3 Resolution	3



Initial response - 06.10.2023 CVE-2023-5217 and CVE-2023-5129

1.1 Affected products: tts performance suite since 2021r2 (producer and QuickAccess / Creator)

1.2 Description

tts wants to inform you about the recently disclosed security vulnerability of the

1.2.1 *"Heap buffer overflow in vp8 encoding in libvpx in Google Chrome prior to 117.0.5938.132 and libvpx 1.13.1 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page"*, source: <https://nvd.nist.gov/vuln/detail/CVE-2023-5217>.

And

1.2.2 *"Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page"*, source: <https://nvd.nist.gov/vuln/detail/CVE-2023-4863>.

We are actively monitoring this problem, and are working on addressing it for all current software installers.

1.3 Resolution

The foreseeable resolution will be, to update the client software to the latest builds. (Producer and QuickAccess). Currently this is being implemented into 2023r2 and then also thereafter merged to the 2023.