

Aggiornamento della sicurezza di VISUCAM ("PrintNightmare")



Aggiornamento della sicurezza di VISUCAM (“PrintNightmare”)

Nota: questo documento non sostituisce il manuale utente fornito con il dispositivo.

Informazioni sull'aggiornamento

“PrintNightmare” è il nome di una vulnerabilità della sicurezza che colpisce i dispositivi con sistemi operativi Microsoft Windows. Secondo Microsoft, “esiste una vulnerabilità legata all'esecuzione di un codice remoto quando il servizio Windows Print Spooler esegue in modo improprio operazioni sui file con determinate autorizzazioni. Sfruttando questa vulnerabilità, un utente malintenzionato potrebbe eseguire un codice arbitrario con privilegi di SYSTEM. Questo potrebbe quindi programmare, visualizzare, modificare o cancellare dati, o creare nuovi account con diritti illimitati”.

“PrintNightmare” non influisce sulla sicurezza o sulla funzionalità di ZEISS VISUCAM 224, VISUCAM 524, VISUCAM 200, VISUCAM 500, VISUCAM PRO NM o VISUCAM NM/FA. Tuttavia, offriamo un aggiornamento di sicurezza (patch) per ZEISS VISUCAM per colmare la vulnerabilità di sicurezza “PrintNightmare”.

Supporto di archiviazione richiesto

VISUCAM 224, 524: chiavetta USB di qualsiasi tipo/capacità di memoria
VISUCAM 200, 500, PRO NM, NM/FA: CD-R (vuoto)

Preparazione

- Scaricare il file zip “CVE-2021-34527.zip”.
- Per VISUCAM 224/524: decomprimere il file zip e salvare il contenuto direttamente nella directory principale della chiavetta USB.
Il file zip è protetto da password. La password è “PrintNightmare”.
- Per VISUCAM 200, 500, PRO NM, NM/FA: decomprimere il file zip e salvare il contenuto direttamente nella directory principale del CD.
Il file zip è protetto da password. La password è “PrintNightmare”.
- Rimuovere tutti i dispositivi esterni collegati tramite USB.
- Scollegare il cavo di rete.



Si prega di eseguire l'aggiornamento immediatamente dopo l'avvio del sistema per evitare il rischio di perdere gli ultimi dati dei pazienti.

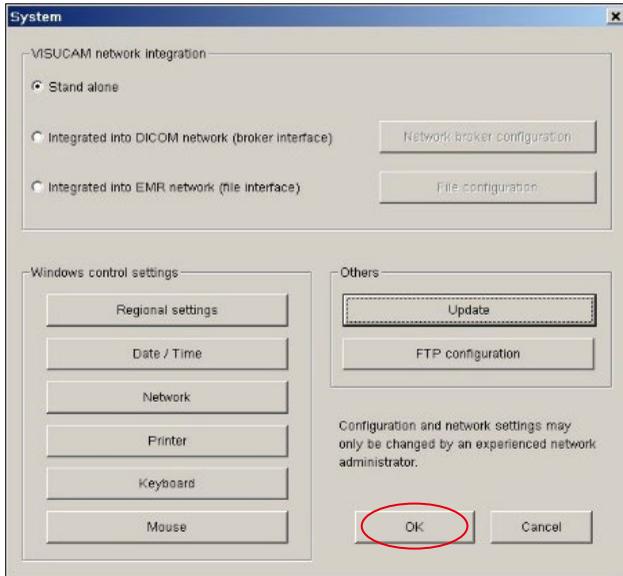
Come installare l'aggiornamento di ZEISS VISUCAM



1. Accendere VISUCAM.
2. Collegare VISUCAM alla chiavetta USB (VISUCAM 224/524) o inserire il CD (VISUCAM200, 500, PRO NM 2, NM/FA 2) sul quale si trova l'aggiornamento scaricato. Potrebbero essere necessari alcuni istanti prima che la chiavetta USB venga installata sul dispositivo.
3. Fare clic su "File" > "System".



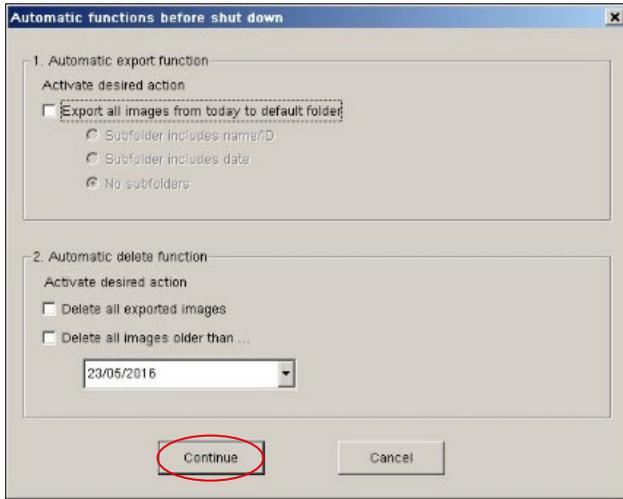
4. Inserire la password di sistema.



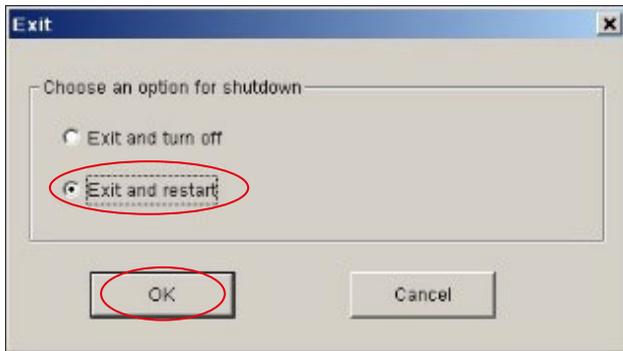
10. Per chiudere la finestra "System" ancora aperta, fare clic su "OK".



11. Una volta completato il processo di installazione, il sistema deve essere riavviato manualmente. Cliccare su "File" > "Exit".

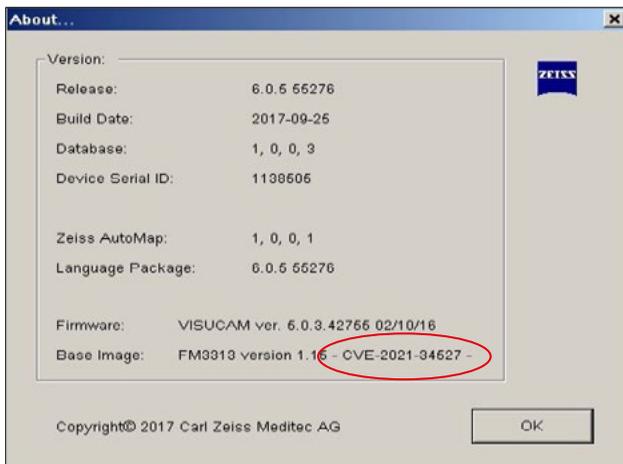


12. Si apre la finestra "Automatic functions...". Continuare facendo clic su "Continue" senza apportare modifiche.



13. La finestra "Exit" si apre di nuovo.

14. Selezionare "Exit and restart". Cliccare su "OK".



15. Dopo aver riavviato il dispositivo, verificare la corretta installazione della patch. Per controllare se l'aggiornamento è stato installato con successo cliccare su "Help" > "About". Verificare che il nome della versione in "Base Image" abbia la seguente estensione: "CVE-2021-34527".

Scopri altri video di esperti, documenti di aiuto, domande e risposte generali su ZEISS Product Insights.



[Sito web ZEISS Product Insights](#)



Carl Zeiss Meditec AG

Göschwitzer Strasse 51-52

07745 Jena, Germania

www.zeiss.com/med

info.meditec@zeiss.com

000000-2133-713-AddG02-IT-260821