Til alle brugere af Artis-systemer, X-Workplace, Sensis- og Arcadis-systemer

Navn: Bue Lars Holm
Afdeling: Healthcare Service
E-mail: bue.lars.holm@siemens-healthineers.com

Dato: 15-06-2017

Vigtig sikkerhedsmeddelelse angående korrigerende handling:

AX038/17/S, AX039/17/S, AX041/17/S, AX042/17/S, AX046/17/S, AX043/17/S

Oplysninger om korrigerende handling for Artis, X-Workplace, Sensis- og Arcadis-systemer for at rette en sårbarhed i Microsoft Windows operativsystemet.

Kære kunde

Formålet med dette brev er at oplyse dig om en korrigerende handling, som vil blive udført for at forhindre en mulig fare for nedbrud.

Hvad er det bagvedliggende problem, som kræver denne korrigerende handling, og hvornår opstår problemet?

Artis, X-Workplace, Sensis- og Arcadis-systemerne benytter operativsystemerne Windows XP og Windows 7. En sårbarhed i disse operativsystemer udgør en sikkerhedsrisiko.
En skadelig software kendt under navnet "WannaCry"-virussen benytter denne sårbarhed til at inficere modtagelige systemer og ødelægge data på disse systemer ved at kryptere dem.

Få flere tekniske oplysninger gennem Siemens Internet-præsentationen:
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-023589.pdf

Hvilken indvirkning er der på systemdriften, og hvor høj er den potentielle risiko?

Den skadelige software krypterer data på inficerede systemer. Hvis dele af Artis-systemet, X-Workplace, Sensis eller Arcadis-systemet krypteres, kan det resultere i en situation, hvor man bliver nødt til at afbryde en klinisk behandling eller overføre den til et velfungerende system.
Som en indirekte virkning kan der også ske tab af data der tidligere er blevet gemt.

Hvilken korrigerende handling vil der blive taget?

Softwaren på de pågældende systemer vil blive opdateret, så den sårbarheden i Microsoft Windows fjernes. Følgende individuelle opdateringer udføres:

AX038/17/S –	ARTIS:	OS HOTFIX-OPDATERING WIN XP SMB SÅRBARHED
AX039/17/S –	ARTIS:	OS HOTFIX-OPDATERING WIN 7 SMB SÅRBARHED
AX041/17/S –	X-WP:	OS HOTFIX-OPDATERING WIN XP SMB SÅRBARHED
AX042/17/S –	X-WP:	OS HOTFIX-OPDATERING WIN 7 SMB SÅRBARHED
AX046/17/S –	SENSIS:	OS HOTFIX-OPDATERING SMB SÅRBARHED
AX043/17/S -	ARCADIS:	OS HOTFIX-OPDATERING WIN XP SMB

Hvordan blev problemet fundet?

– Truslen blev identificeret, da man konstaterede, at visse systemer i den private og industrielle sektor samt sundhedssektoren var inficerede. Man må gå ud fra at Artis, X-Workplace, Sensis- og Arcadis-systemerne har en tilsvarende sårbarhed. Indtil nu er der konstateret ét isoleret tilfælde, hvor et Sensis-system er blevet inficeret.

Hvor effektive er de korrigerende foranstaltninger?

Softwaren eliminerer årsagen, og forebygger dermed angreb fra "WannaCry"-ransomwaren eller anden skadelig software der benytter de sårbarheder i MS Windows, som denne hotfix afhjælper.

Hvordan vil den korrigerende handling blive udført?

Software-opdateringen vil blive gennemført som en remote-opdatering. Hvor dette ikke er muligt, vil vores serviceafdeling snarest kontakte dig for at aftale en dato for udførelse opdateringen. Du er velkommen til at kontakte vores serviceafdeling med henblik på en tidligere aftale. Dette brev vil blive sendt til alle berørte kunder som opdatering **AX037/17/S**.

Hvilke risici er der for patienter, som tidligere er blevet undersøgt eller behandlet med dette system?

I dette tilfælde finder vi det ikke nødvendigt at foretage en ny undersøgelse af patienterne. Dette er en mulig defekt, der ikke havde indflydelse på behandlingen af patienterne.

Vi takker for dit samarbejde med hensyn til denne sikkerhedsmeddelelse og beder om, at du straks meddeler og instruerer alle medarbejdere i din organisation, som skal have kendskab til dette problem. Send også sikkerhedsoplysningerne til andre organisationer, der kan tænkes at blive påvirket.

Hvis enheden er blevet solgt og derfor ikke længere er i din besiddelse, bedes du sende denne sikkerhedsmeddelelse til den nye ejer. Vi vil også bede dig om så vidt muligt at oplyse os om den nye ejers identitet.

Venlig hilsen

Siemens Healthcare A/S