ADVISORY : MEERDERE KWETSBAARHEDEN IN SIEMENS MOLECULAIRE BEELDVORMINGSAPPARATEN (PET/CT/SPECT SYSTEMEN)

Referentie: CERT.be Advisory #2017-005
Versie: 1.0

Doelpubliek: ziekenhuizen, medische centra, tandartsen enz die Windows 7-gebaseerde versies van SIEMENS PET/CT en SPECT/CT hebben

Geïmpacteerde software: Alle Windows 7-gebaseerde versies van Siemens PET/CT/SPECT Systemen, alle Windows 7 SPECT Werkplaatsen / Sybmia.net, Mobilett Mira Max: All versies voor VE10S without XP009/17/S
Type: Programmacode kan uitgevoerd worden onder de rechten van de lokale gebruiker

Bronnen

https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-822184.pdf
https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-131263.pdf

Risico's

Succesvolle exploitatie van deze kwetsbaarheden geeft de aanvaller de mogelijkheid om willekeurige programmacode uit te voeren met de rechten van een lokale gebruiker, dit kan volledige toegang verschaffen van het systeem aan de aanvaller. (vb. het stelen of modificeren van patiënten informatie, veranderingen aan de configuratie,…)

Deze kwetsbaarheden hebben een CVSS v3 score gekregen van 9.8 op 10. De impact van deze kwetsbaarheden hangt af van veel factoren die uniek zijn voor iedere organisatie.

Samenvatting

Siemens heeft meerdere kwetsbaarheden geïdentificeerd in Siemens Moleculaire beeldvormingsproducten die gebaseerd zijn op Windows 7. Siemens vermeldt ook dat er meerdere kwetsbaarheden zijn in de Mobilett Mira Max – mobiele digitale X-ray systemen.

Deze kwetsbaarheden kunnen van op afstand misbruikt worden. Exploits voor deze kwetsbaarheden zijn publiek beschikbaar en hebben een minimum aan inspanning nodig om uitgevoerd te worden.

Geïmpacteerde producten:

- Siemens PET/CT Systemen: Alle Windows 7-gebaseerde versies
- Siemens SPECT/CT Systemen: Alle Windows 7-gebaseerde versies
- Siemens SPECT Systemen: Alle Windows 7-gebaseerde versies
- Siemens SPECT Workplaces / Symbia.net: Systemen: Alle Windows 7-gebaseerde versies

- Mobilett Mira Max: Alle versies voor VE10S zonder update XP009/17/S

Voor de CT/PET/SPECT systemen gebaseerd op Windows 7:

Kwetsbaarheid CVE-2015-1635:

Een niet-geverifieerde externe aanvaller kan willekeurige code uitvoeren door speciaal vervaardigde HTTP-verzoeken naar de Microsoft-webserver (poort 80 / tcp en poort 443 / tcp) van geïmpacteerde systemen te verzenden.

Kwetsbaarheid CVE-2015-1497:

Een niet-geverifieerde externe aanvaller kan willekeurige code uitvoeren door een speciaal vervaardigd verzoek naar de HP Client-automatiseringsdienst te verzenden op poort 3465 / tcp van geïmpacteerde apparaten.

Kwetsbaarheden CVE-2015-7860 / 7861:

Een niet-geverifieerde externe aanvaller kan willekeurige code uitvoeren door een speciaal vervaardigd verzoek naar de HP Client-automatiseringsdienst te verzenden van geïmpacteerde apparaten.

Voor de Mobilett Mira Max systemen

Kwetsbaarheden CVE-2017-0143 / 0144 / 0145 / 0146 / 0147 / 0148:

Een niet-geverifieerde externe aanvaller kan willekeurige code uitvoeren door een speciaal vervaardigd verzoek verzonden naar de SMBv1 server van de geïmpacteerde Microsoft Windows systemen.

Aanbevolen acties

Voor de CT/PET/SPECT systemen gebaseerd op windows 7:

Siemens werkt aan updates voor de geïmpacteerde producten en raadt aan om de netwerktoegang tot de moleculaire beeldvormingsproducten met afdoende maatregelen te beveiligen.

Zolang deze updates nog niet uitgebracht zijn, adviseert Siemens om deze apparaten te gebruiken in een afgescheiden (dedicated) netwerksegment in een afdoende beschermde IT-omgeving.

Voor de Mobilett Mira Max: Alle versies voor VE10S zonder XP009/17/S :

Siemens levert software update XP009 / 17 / S voor ondersteunde versies van Mobilett Mira Max voor VE10S.

De update is automatisch beschikbaar voor klanten met ondersteuning op afstand. Als er geen externe ondersteuning beschikbaar is of voor vragen over de update procedure, kunt u contact opnemen met Siemens Klantendienst.

Tot wanneer de updates beschikbaar zijn en voor end-of-support producten, beveelt Siemens aan om de getroffen producten die luisteren op netwerkpoorten 139/tcp, 445/tcp of 3389/tcp van elk geïnfecteerd systeem in zijn respectieve netwerk segment te isoleren (bijv. Door het blokkeren van toegang tot bovenstaande netwerk poorten via de firewall.)

Indien dit niet mogelijk is, raadt Siemens het volgende aan:

- Als de veiligheid van de patiënt en de behandeling niet in gevaar is, verwijder het apparaat dan van het netwerk en gebruik het in autonome werking.

- Verbind het product enkel maar terug met het netwerk nadat de update geïnstalleerd is op het system. Siemens beschikt over de mogelijkheid om systemen die in staat zijn tot Remote Update Handling (RUH) veel sneller bij te werken dan door een interventie ter plaatse. Klanten van RUH apparatuur krijgen de aanbeveling om de situatie over de beschikbaarheid van patches en resterende risico's in het netwerk met de Siemens klantendienst te verduidelijken. Nadien moeten ze dan hun systemen opnieuw verbinden om zo snel mogelijk updates te ontvangen via Remote Update Handling. Dit zorgt voor een vlotte en snelle ontvangst van updates en ondersteunt het herstel van systeemoperaties.

Siemens raadt ook het volgende aan:

- Verzeker dat u passende back-ups en systeemherstelprocedures hebt.

- Voor specifieke informatie over updates en remediëring kunt u contact opnemen met uw lokale Siemens Klantenservice engineer of een regionaal ondersteuningscentrum.

CERT.be beveelt ook aan dat organisaties defensieve maatregelen nemen om het risico te minimaliseren, onder andere:

- Minimaliseer netwerktoegang voor alle medische apparaten en/of systemen en verzeker u dat deze niet beschikbaar zijn vanaf het internet.

- Plaats alle medische apparaten en externe apparaten achter firewalls en isoleer deze van het bedrijfsnetwerk.

Wanneer externe toegang nodig is, gebruik dan beveiligde methodes, zoals Virtuele Private Netwerken (VPN's). Herken ook het risico in VPN's, deze kunnen ook kwetsbaarheden bevatten en moeten bijgewerkt worden naar de meest recente versie. Weet ook dat een VPN net zo veilig is als de aangesloten apparaten.

Referenties

Meer informatie over deze beveiligingslekken en gedetailleerde mitigatie-instructies, vindt u in de Siemens Security Advisory SSA-814457 / 131263 op de volgende locatie:

http://www.siemens.com/cert/advisories