بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

آسیب‌پذیری TightVNC و تاثیر آن بر روی محصولات Siemens

آسیب‌پذیری

شناسه سند ..... MaherReport_13991010-01
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۱۰/۰۹
طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی، نرسیده به قائم مقام فراهانی، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران

42650000 (021)

42650000 (021)

cert.ir

فهرست مطالب

1 آسیب‌پذیری TightVNC و تاثیر آن بر روی محصولات Siemens ۱

۱ آسیب‌پذیری TightVNC و تاثیر آن بر روی محصولات Siemens

چندین آسیب‌پذیری در محصولات نسخه 1.x از TightVNC وجود دارد که امکان اجرای کد از راه دور و حمله انکار سرویس را در شرایط خاص فراهم می‌آورند. Siemens برای چندین محصول خود که تحت تاثیر آسیب‌پذیری‌های TightVNC هستند، به‌روزرسانی ارئه کرده است و در حال تلاش برای به‌روزرسانی سایر محصولات تحت تاثیر آسیب‌پذیری است.

راهکار پیشنهادی Siemens برای جلوگیری از سوءاستفاده از این آسیب‌پذیری‌ها در محصولاتی که هنوز به‌روزرسانی برای آنها ارائه نشده است، محدود کردن دسترسی به محصول آسیب‌پذیر می‌باشد. لذا توصیه می‌شود، چنانچه یکی از محصولات آسیب‌پذیری Siemens را که هنوز به‌روزرسانی نشده است، استفاده می‌کنید؛ سریعا دسترسی به محصول را به شبکه داخلی یا شبکه VPN و فقط به آدرس‌های IP معتبر محدود نمایید.

جدول ۱ محصولات از Siemens که تحت آسیب‌پذیری‌های TightVNC (v1.X) قرار دارند و راه حل در نظر گرفته شده برای این محصولات را نمایش می دهد.

جدول ۱- محصولات تحت تاثیر آسیب‌پذیری

محصول تحت تاثیر آسیب‌پذیری	راه حل
SIMATIC HMI Comfort Outdoor Panels 7” and 15” (شامل انواع SIPLUS) تمام نسخه‌های قبل از Version 16 update 3	به روزرسانی SIMATIC WinCC (TIA Portal) به نسخه V16 Update 3 یا نسخه های جدیدتر و سپس به روزرسانی پنل به V16 Update 3 یا نسخه‌های جدیدتر
SIMATIC HMI Comfort Panel 4” to 22”(شامل انواع SIPLUS) تمام نسخه‌های قبل از Version 16 update 3	به روزرسانی SIMATIC WinCC (TIA Portal) به نسخه V16 Update 3 یا نسخه های جدیدتر و سپس به روزرسانی پنل به V16 Update 3 یا نسخه‌های جدیدتر
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F تمام نسخه‌های قبل از Version 16 update 3	به روزرسانی SIMATIC WinCC (TIA Portal) به نسخه V16 Update 3 یا نسخه های جدیدتر و سپس به روزرسانی پنل به V16 Update 3 یا نسخه‌های جدیدتر
SIMATIC ITC1500 v3.1 تمام نسخه‌ها	محدود سازی دسترسی به محصول

محصول تحت تاثیر آسیب‌پذیری	راه حل
SIMATIC ITC1500 v3.1 PRO تمام نسخه‌ها	محدود سازی دسترسی به محصول
SIMATIC ITC1900 v3.1 تمام نسخه‌ها	محدود سازی دسترسی به محصول
SIMATIC ITC1900 v3.1 PRO تمام نسخه‌ها	محدود سازی دسترسی به محصول
SIMATIC ITC2200 v3.1 تمام نسخه‌ها	محدود سازی دسترسی به محصول
SIMATIC ITC2200 v3.1 PRO تمام نسخه‌ها	محدود سازی دسترسی به محصول
SIMATIC WinCC Runtime Advanced تمام نسخه‌های قبل از Version 16 update 3	محدود سازی دسترسی به محصول
SIMATIC WinCC Runtime Professional تمام نسخه‌های قبل از Version 16 update 3	محدود سازی دسترسی به محصول

سه مورد از آسیب‌پذیری‌های TightVNC دارای درجه اهمیت بحرانی و یک مورد دارای درجه اهمیت بالا است. لیست آسیب‌پذیری‌های TightVNC در جدول ۲ ارائه شده است.

جدول ۲- آسیب‌پذیری‌های TightVNC

شناسه آسیب‌پذیری	نوع آسیب‌پذیری	نسخه های تحت تاثیر	شدت آسیب‌پذیری
CVE-2019-15678	اجرای کد از راه دور	نسخه 1.3.10	۹,۸
CVE-2019-15679	انکار سرویس	نسخه 1.3.10	۹,۸
CVE-2019-15680	اجرای کد از راه دور	نسخه 1.3.10	۷,۵
CVE-2019-8287	اجرای کد از راه دور	نسخه 1.3.10	۹,۸

منبع:

https://cert-portal.siemens.com/productcert/pdf/ssa-478893.pdf

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-08