باسمه تعالی

عنوان مستند

آسیب پذیری بهره برداری محلی از محصولات صنعتی زیمنس

فهرست مطالب

۱ چکیده

در پیکربندی های غیر پیش فرض، چندین محصول صنعتی، به وسیله یک آسیب پذیری تحت تأثیر قرار گرفته اند که این آسیب پذیری می تواند به کاربران محلی سیستم عامل مایکروسافت ویندوز اجازه دهد امتیازات خود را تحت شرایط خاص افزایش دهد. این محصولات عبارتند از:

- SIMATIC WinCC یک سیستم SCADA است.
- SIMATIC STEP 7 V5.X و SIMATIC STEP 7 (TIA Portal)، محصولات نرم افزار مهندسی برای محصولات SIMATIC PLC هستند.
- SIMATIC PCS 7 یک سیستم کنترل توزیع شده (DCS) است که SIMATIC WinCC را تکمیل می کند.
- SIMATIC WinCC Runtime Professional یک پلت فرم مجازی سازی Runtime است که برای کنترل اپراتور و نظارت بر دستگاه ها و کارخانه ها مورد استفاده قرار می گیرد.
- SIMATIC WinCC (TIA Portal) یک نرم افزار مهندسی است که برای پیکربندی و برنامه ریزی پنل های SIMATIC، PCهای صنعتی SIMATIC و PCهای استاندارد که نرم افزار مجازی سازی WinCC Runtime Advanced یا SCADA System WinCC Runtime Professional را اجرا می کنند، به کار می رود.
- SIMATIC NET PC-Software برای ارتباط بین کنترلرها (PLCها) و رویه های مبتنی بر PC (HMIها) استفاده می شود.
- SINEMA Remote Connect Client، مدیریت اتصالات ایمن (VPN) را بین مراکز، تکنسین های خدماتی و دستگاه های نصب شده یا کارخانه ها تضمین می کند.
- SINEMA Server، نرم افزار مدیریت شبکه برای استفاده در شبکه های اترنت صنعتی است.
- SIMATIC WinCC RTX، کنترلر نرم افزار SIMATIC برای رویه های اتوماسیون مبتنی بر PC است.
- SIMATIC IT Production Suite، رویه IT متمرکز بر کارخانه است که ارتباط بین سیستم های تجاری (مانند ERP) و سیستم های کنترل را ایجاد می کند.
- TeleControl Server Basic اجازه نظارت از راه دور و کنترل کارخانه ها را می دهد.
- SOFTNET Security Client، به دستگاه های برنامه نویسی مانند PCها و کامپیوترهای نوت بوک اجازه می دهد به گره های شبکه یا سیستم های اتوماسیون محافظت شده توسط SCALANCE S دسترسی داشته باشند.

- نرم افزار شبیه سازی SIMIT، به منظور پیش بینی خطاها در اوایل فاز برنامه ریزی، اجازه شبیه سازی کارخانه را می دهد.
- Security Configuration Tool (SCT) یک نرم افزار مهندسی برای دستگاه های امنیتی مانند SCALANCE S یا CP 443-1 Advanced است.
- Primary Setup Tool (PST)، اجازه پیکربندی اولیه شبکه محصولات SIMATIC NET Industrial Ethernet را می دهد.

براساس گفته های زیمنس، این محصولات در سرتاسر چندین بخش از جمله سیستم های پتروشیمی، انرژی، مواد غذایی و کشاورزی، آب و فاضلاب بکار گرفته شده اند.

شرکت زیمنس، بروزرسانی هایی را برای برخی محصولات و وصله موقتی را برای بقیه محصولات تحت تأثیر، ارائه می کند. این شرکت در حال فعالیت روی نسخه های جدیدی برای بقیه محصولات تحت تأثیر می باشد.

۲ محصولات تحت تأثیر

نسخه های تحت تأثیر این آسیب پذیری عبارتند از:

- SIMATIC WinCC
  - V7.0 SP2 و نسخه های ماقبل V7.0 SP2 Upd 12
  - V7.0 SP3: تمام نسخه های ماقبل V7.0 SP3 Upd 8
  - V7.2: تمام نسخه ها
  - V7.3: تمام نسخه ها
  - V7.4: تمام نسخه ها
- SIMATIC STEP 7 V5.X: تمام نسخه ها
- SIMATIC PCS 7
  - V7.1 و نسخه های ماقبل
  - V8.0: تمام نسخه ها
  - V8.1: تمام نسخه ها
  - V8.2: تمام نسخه ها
- SIMATIC WinCC Runtime Professional: تمام نسخه ها
- SIMATIC WinCC (TOA Portal) Professional: تمام نسخه ها
- SIMATIC WinCC (TIA Portal) Basic, Comfort, Advanced: تمام نسخه های ماقبل V14
- SIMATIC STEP 7 (TIA Portal): تمام نسخه های ماقبل V14
- SIMATIC NET PC-Software: تمام نسخه های ماقبل V14

- SINEMA Remote Connect Client: تمام نسخه ها
- SINEMA Server: تمام نسخه های ماقبل V13 SP2
- SIMATIC WinAC RTX 2010 SP2: تمام نسخه ها
- SIMATIC WinAC RTX F 2010 SP2: تمام نسخه ها
- SIMATIC IT Production Suite: تمام نسخه ها
- TeleControl Server Basic: تمام نسخه ها
- SOFTNET Security Client V5.0: تمام نسخه ها
- SIMIT V9.0
- Security Configuration Tool (SCT): تمام نسخه ها
- Primary Setup Tool (PST): تمام نسخه ها

۳ تأثیر آسیب پذیری

این آسیب پذیری می تواند به کاربران محلی اجازه دهد امتیازات خود را ارتقا دهند، در صورتی که محصولات تحت تأثیر، در مسیر پیش فرض نصب نشده باشند.

تاثیر این آسیب پذیری بر سازمان ها به فاکتورهای متعددی که برای هر سازمان منحصر به فرد هستند، بستگی دارد. NCCIC/ICS-CERT به سازمان ها توصیه می کند تاثیر این آسیب پذیری را بر اساس محیط عملیاتی، معماری و پیاده سازی محصول شان ارزیابی کنند.

۴ مشخصه های آسیب پذیری

۴-۱ مروری بر آسیب پذیری

۴-۱-۱ مدیریت نامناسب امتیاز

ممکن است مسیرهای قید نشده سرویس، به کاربران محلی سیستم عامل مایکروسافت ویندوز اجازه دهد امتیازات خود را ارتقا دهند، در صورتی که محصولات تحت تأثیر، در مسیر پیش فرض خود نصب نشده باشند («C:\Program Files*» یا مسیری مشابه).

این آسیب پذیری CVE-2016-7165 نام گذاری شده است. نمره CVSS v3 پایه 6.4 به آن اختصاص داده شده است و رشته برداری CVSS آن «AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H» می باشد.

۴-۲ جزئیات آسیب پذیری

۴-۲-۱ قابلیت بهره برداری

این آسیب پذیری از راه دور قابل بهره برداری نبوده و فقط توسط یک کاربر معتبر و محلی سیستم عامل قابل بهره برداری است

۴-۲-۲ بهره برداری موجود

هیچ گونه بهره برداری شناخته شده ای این آسیب پذیری را هدف قرار نمی دهد.

۴-۲-۳ سطح آسیب پذیری

ایجاد یک بهره برداری کارکننده برای این آسیب پذیری، بسیار مشکل خواهد بود.

۵ اقداماتی جهت کاهش شدت آسیب پذیری ها

در صورتی که محصولات تحت تأثیر، در مسیر پیش فرض خود نصب شده باشند («C:\Program Files*» یا مسیری مشابه) و مجوزهای پیش فرض دسترسی به سیستم فایل برای درایو «C:\» تغییر نکرده باشد، این آسیب پذیری امنیتی قابل بهره برداری نیست.

با این وجود، در صورتی که محصولات تحت تأثیر در مسیر پیش فرض خود نصب نشده باشند («C:\Program Files*» یا مسیری مشابه)، احتمال بهره برداری از آسیب پذیری امنیتی وجود دارد.

شرکت زیمنس، بروزرسانی هایی را برای محصولات زیر منتشر کرده و کاربران را تشویق می کند هر چه سریع تر از این بروزرسانی ها استفاده کنند:

- SIMATIC WinCC:
  - V7.0 SP2 و نسخه های ماقبل: بروزرسانی به V7.0 SP2 Upd 12
  - V7.0 SP3: بروزرسانی به V7.0 SP3 Upd 8
- SIMATIC WinCC (TIA Portal) Basic, Comfort, Advanced: ارتقا به V14
- SIMATIC STEP 7 (TIA Portal): ارتقا به V14
- SIMATIC NET PC-Software: ارتقا به V14
- TeleControl Server Basic: بروزرسانی به V3.0 SP2
- SINEMA Server: بروزرسانی به V13 SP2

برای محصولات زیر در پیکربندی های غیر پیش فرض، زیمنس وصله موقتی ارائه کرده که آسیب پذیری امنیتی را برطرف می کند:

- SIMATIC WinCC V7.2
- SIMATIC STEP 7 V5.X
- SIMATIC PCS 7 V7.1 & V8.0
- SIMATIC STEP 7 (TIA Portal) V13
- SIMATIC NET PC-Software V13
- SINEMA Remote Connect Client
- SIMATIC WinAC RTX 2010 SP2
- SIMATIC WinAC RTX F 2010 SP2
- SIMATIC IT Production Suite
- SOFTNET Security Client V5.0
- SIMIT V9.0
- Security Configuration Tool (SCT)
- Primary Setup Tool (PST)

برای محصولات زیر در پیکربندی های غیر پیش فرض، زیمنس به کاربران پیشنهاد می کند که از وصله موقتی استفاده کرده، از دستورالعمل های عملیاتی شرکت زیمنس پیروی کرده و امتیازات دسترسی به سیستم فایل را محدود کنند:

- SIMATIC WinCC V7.3 & V7.4
- SIMATIC PCS 7 V8.1 & V8.2
- SIMATIC WinCC Runtime Professional
- SIMATIC WinCC (TIA Portal) Professional

شرکت زیمنس به شدت به توصیه می کند که کاربران از دسترسی شبکه به ایستگاه های کاری مهندسی و فضای ذخیره سازی پروژه با مکانیزم های مناسب محافظت کنند. همچنین پیشنهاد می کند که کاربران محیط عملیاتی را براساس راهنمای عملیاتی امنیت صنعتی شرکت زیمنس پیکربندی کنند.

ICS-CERT جهت حفاظت در برابر این آسیب پذیری و دیگر خطرات امنیت سایبری، به کاربران توصیه می کند تدابیر امنیتی بیشتری در نظر گیرند. به طور خاص، کاربران باید:

- در معرض شبکه قرار گرفتن تمام دستگاه های سیستم و/یا سیستم های کنترل را به حداقل برسانند، و مطمئن شوند که آنها از طریق اینترنت قابل دسترسی نیستند.
- شبکه های سیستم کنترل و دستگاه های راه دور را در پشت دیوارآتش مستقر سازند، و آن ها را از شبکه تجاری جدا سازند.
- هنگامی که دسترسی از راه دور مورد نیاز است، از روش های امن، مانند شبکه های خصوصی مجازی (VPNs) استفاده کنند، در نظر داشته باشند که VPNها نیز ممکن است آسیب پذیری هایی داشته

باشند و باید به جدیدترین نسخه موجود به روز رسانی شوند. همچنین VPN تنها امنیت دستگاه های متصل را تأمین می کند.

ICS-CERT یادآور می شود که سازمان ها قبل از اعمال تدابیر امنیتی، آنالیز مناسبی از تأثیر و ارزیابی خطر انجام دهند.

۶ منابع

- https://ics-cert.us-cert.gov/advisories/ICSA-16-313-02
- http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-701708.pdf