باسمه تعالی

عنوان مستند

آسیب پذیری انکار سرویس[1] در محصولات
SICAM RTU شرکت زیمنس

[1] Denial-of-Service

فهرست مطالب

۱ چکیده

واحد ترمینال راه دور (RTU)، یک دستگاه الکترونیکی تحت کنترل ریزپردازنده است که از طریق انتقال اطلاعات دورسنجی به یک سیستم مرکزی و با استفاده از پیام های سیستم نظارت مرکزی برای کنترل اشیای به هم متصل، رابط بین اشیا در دنیای فیزیکی و یک سیستم کنترلی توزیع شده یا سیستم SCADA می باشد. عبارات دیگری که ممکن است برای RTU به کار رود، «واحد دورسنجی» یا «واحد کنترل راه دور» است.

RTU بر پارامترهای میدانی دیجیتال و آنالوگ نظارت کرده و داده ها را به ایستگاه نظارت مرکزی ارسال می کند. RTU حاوی نرم افزار راه اندازی برای اتصال جریان های ورودی اطلاعات به جریان های خروجی اطلاعات، برای تعریف پروتکل های ارتباطی و عیب یابی مشکلات راه اندازی می باشد.

از RTUها برای نظارت در صنایعی مانند نفت و گاز (پلت فرم های خارج از خشکی، چاه های نفت درون خشکی)، شبکه های ایستگاه پمپ (جمع آوری فاضلاب یا تأمین آب)، سیستم های نظارت محیطی (آلودگی، کیفیت هوا، نظارت تشعشعات)، معدن ها، تجهیزات ترافیک هوایی مانند کمک های جهت یابی استفاده می شود.

همچنین از آنها برای نظارت و کنترل فعالیت هایی مانند آب نگاری (سیستم های تأمین آب، مخازن، فاضلاب)، شبکه های انتقال نیروی برق و تجهیزات مربوطه، شبکه های گاز طبیعی و تجهیزات مربوطه و آژیرهای هشدار خارجی نیز استفاده می شود.

ماژول های ارتباطی SM-2558 و SM2556 شرکت زیمنس، معیارهای پروتکل برای ارتباط LAN/WAN همراه با رابط اترنت سریع هستند.

آخرین سفت افزار ETA4 برای ماژول ارتباطی SM-2558 IEC 60870-5-140، یک آسیب پذیری را برطرف می سازد که می توانست به مهاجمان راه دور اجازه دهد حمله انکار سرویس را تحت شرایط خاصی اجرا کنند.

۲ محصولات تحت تأثیر

- سفت افزار ETA4 (تمام نسخه های قبل از بازبینی 08) از ماژول افزونه SM-2558 در محصولات زیر آسیب پذیر است:
  - SICAM AK
  - SICAM TM 1703
  - SICAM BC 1703
  - SICAM AK 3
- سفت افزار ETA4 (بازبینی 11.01 و ماقبل) از ماژول افزونه SM-2556 در محصولات زیر آسیب پذیر است:
  - SICAM AK
  - SICAM TM
  - SICAM BC

۳ تأثیر آسیب پذیری

بهره موفق از این آسیب پذیری می تواند باعث حمله انکار سرویس شود. ممکن است برای بازیابی سیستم، راه اندازی در دمای اتاق مورد نیاز باشد.

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 انکار سرویس

بسته های طراحی شده و خاص که به درگاه 2404/TCP ارسال شده، می تواند باعث شود فعالیت دستگاه تحت تأثیر، دچار نقص گردد. ممکن است راه اندازی در دمای محیط برای بازیابی سیستم مورد نیاز باشد.

این آسیب پذیری CVE-2016-7987 نام گذاری شده است. نمره CVSS v3 پایه 7.5 به آن اختصاص داده شده است و رشته برداری CVSS آن «AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H» می باشد.

۴-۲ جزئیات آسیب پذیری

۴-۲-۱ قابلیت بهره برداری

بهره برداری از این آسیب پذیری می تواند از راه دور انجام شود.

۴-۲-۲ بهره برداری موجود

مشخصاً هیچ گونه بهره برداری شناخته شده و عمومی، این آسیب پذیری را هدف قرار نمی دهد.

۴-۲-۳ سطح آسیب پذیری

یک مهاجم با سطح مهارت پایین، قادر به بهره برداری از این آسیب پذیری می باشد.

۵ اقداماتی جهت کاهش شدت آسیب پذیری ها

شرکت زیمنس، سفت افزار ETA4 Revision 08 را برای SM-2558 ارائه می کند که آسیب پذیری را برطرف کرده و به کاربران پیشنهاد می کند که به نسخه تصحیح شده بروزرسانی کنند.

برای ماژول افزونه SM-2556، شرکت زیمنس به مشتریان پیشنهاد می کند با پشتیبانی شرکت ارتباط برقرار کنند.

تا زمان بکارگیری وصله ها، زمینس توصیه می کند اقدامات زیر برای کاهش شدت آسیب پذیری اتخاذ شوند:

- استفاده از دیوار آتشین یا قابلیت IPsec ماژول SM-2558 به منظور محدود کردن دسترسی به درگاه 2404/TCP.
- دستورالعمل امنیتی مدیریت RTUهای SICAM.

- RTUها همیشه در شبکه های مطمئن اجرا شوند.

به عنوان یک معیار کلی امنیتی، زیمنس به شدت توصیه می کند از دسترسی به شبکه، با مکانیزم های مناسب محافظت شود (برای مثال، دیوارهای آتش، قسمت بندی، VPN). توصیه می شود محیط براساس دستورالعمل های عملیاتی شرکت زیمنس پیکربندی گردد تا دستگاه ها در محیط ایمن اجرا شوند.

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-16-299-01
- https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-296574.pdf