# گزارش آسیب پذیری

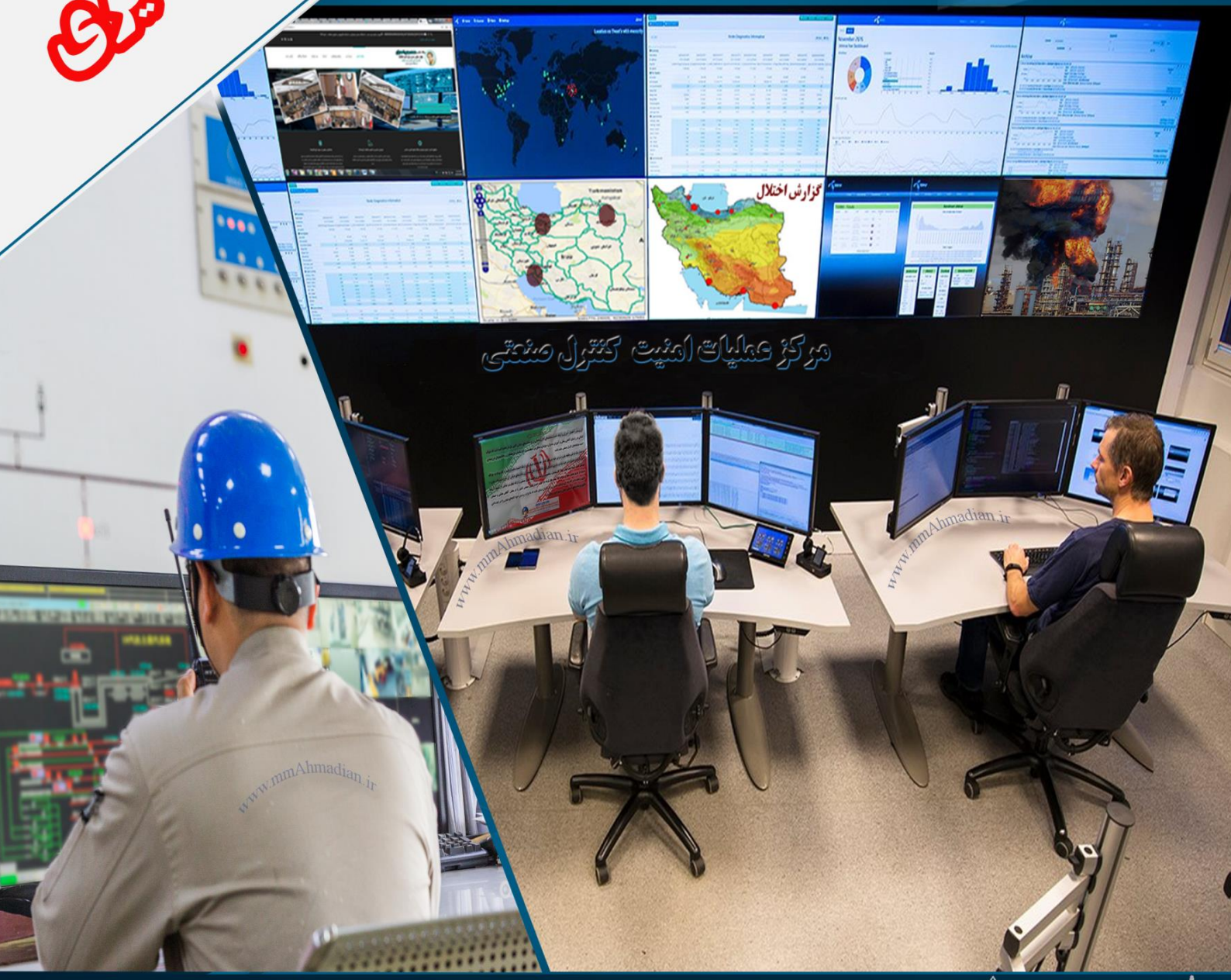
# CVE-2018-5459

سطح مخاطره : حیاتی

محصول تحت تأثیر: WAGO PFC200

نسخه سند: ۱,۰,۲

تاریخ انتشارعمومی سند: ۹۷/۲/۶




نفت و گاز | پالایش و پتروشیمی | آب و فاضلاب | فولاد و مس | هسته ای | برق و انرژی | سایر صنایع و کارخانه ها


@MohammadMehdiAhmadian
www.mmAhmadian.ir
@mmAhmadian

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


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



بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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. مشخصات آسیب‌پذیری

جدول ۱: مشخصات آسیب‌پذیری

| | |
|---|---|
| شناسه آسیب‌پذیری: | CVE-2018-545 |
| محصول تحت تأثیر: | کنترل‌کننده WAGO PFC200 متأثر از نرم‌افزار 3S CoDeSys Runtime |
| تاریخ گزارش آسیب‌پذیری | (ICS-Cert)2018 February 14 |
| تاریخ گزارش آسیب‌پذیری توسط سازنده: | 2017 December 7 |
| نوع آسیب‌پذیری: | احراز اصالت[1] نامناسب (درنتیجه امکان دسترسی غیرمجاز از راه دور) |
| سطح مخاطره: | حیاتی |
| نمره CVSS[2]: | 9.8 |

# ۲. معرفی آسیب‌پذیری

اخیراً آسیب‌پذیری از نوع احراز اصالت نامناسب در نرم‌افزار CoDeSys[3] شناسایی شد که محصولات WAGO PFC200 را تحت تأثیر قرار می‌دهد. این آسیب‌پذیری این امکان را به مهاجمین می‌دهد که در صورت بهره‌جویی[4] موفق بتوانند به شکل غیرمجاز به کنترل‌کننده (PLC) وصل شده و انواع دستورات و عملیات غیرمجاز را به شکل راه دور و از طریق درگاه[5] TCP شماره ۲۴۵۵ انجام دهند؛ این دستورات شامل خواندن، نوشتن و پا کردن فایل یا دست‌کاری برنامه کنترل‌کننده (PLC) در حین اجرا است.

# ۳. گزاش فنی آسیب‌پذیری

[1] Authentication(تصدیق اصالت یا احراز اصالت)

[2] Common Vulnerability Scoring System

[3] controller development system

[4] Exploit

[5] Port

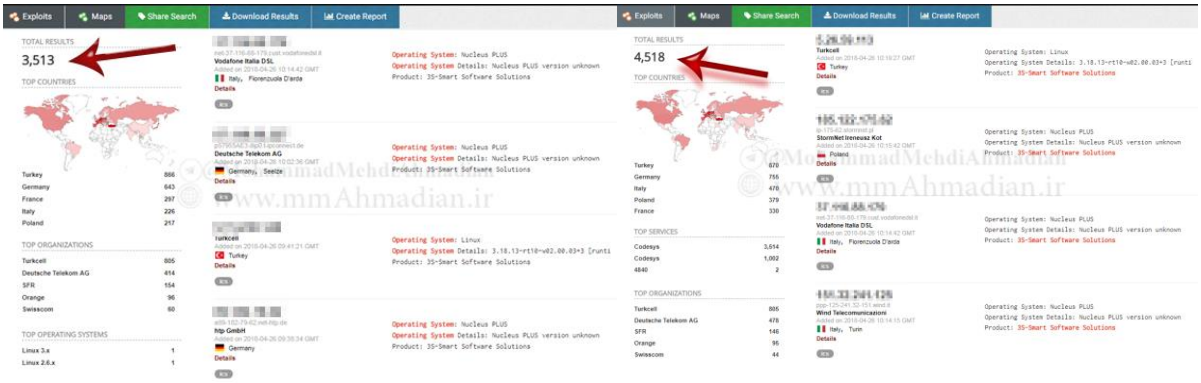
بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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

نرم‌افزار CoDeSys در سال‌های اخیر دارای آسیب‌پذیری‌های متعددی بوده است که به شکل عمومی منتشرشده‌اند و در محافل مختلف در مورد آسیب‌پذیری‌های آن بحث شده است (تعدادی از آسیب‌پذیری‌های مهم این نرم‌افزار در بخش ۶ آورده شده است). قابل توجه است که نرم افزار CoDeSys در هر دو سیستم عامل ویندوز و لینوکس استفاده می‌شود با انواع خانواده‌های پرداشگر از جمله x86، MIPS، ARM و غیره و با انواع پروتکل‌های کنترل صنعتی از جمله مدباس، پروفی‌نت، اترنت/آی پی و غیره کار می‌کند؛ همین باعث شده است که به همراه کنترل‌کننده‌های عمومی WAGO در بسیاری از صنایع دنیا استفاده شود.

آسیب‌پذیری CVE-2018-545 برای اولین بار توسط Reid Wightman گزارش شد. درگاه ۲۴۵۵ در شبکه‌های هدف برای انتقال برنامه از کارگزار[1] به PLC انجام می‌شود و باید بعد از راه‌اندازی اولیه بسته شود. قابل‌توجه است که غالباً درگاه TCP شماره ۲۴۵۵ در سامانه‌هایی که نرم‌افزار CoDeSys متصل به کنترل‌کننده نصب می‌شود به شکل پیش‌فرض باز است. این حمله هر سه اصل امنیتی محرمانگی، صحت و دسترس‌پذیری نرم‌افزار CoDeSys و کنترل‌کننده هدف را می‌تواند نقض کند (این سه اصل در ضمیمه ج توضیح داده‌شده‌اند).

در تاریخ تهیه این گزارش، در بازه‌ی ۴۵۱۸ -۳۵۱۳ قلم تجهیز صنعتی متصل به اینترنت با درگاه باز ۲۴۵۵ شناسایی شدند که خوشبختانه در بخش کنترل صنعتی کشور ما، موردی رصد نشد.




## ۴. محصولات تحت تأثیر

نسخه‌های ذیل از نرم‌افزار 3S CoDeSys Runtime از خانواده PFC200:

- CoDeSys Version 2.3.X
- CoDeSys Version 2.4.X

[1] Server

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

نسخه‌های سفت افزار[1] WAGO PFC200 قبل از نسخه (10)02.07.07:

- 750-8202,
- 750-8202/025-000,
- 750-8202/025-001,
- 750-8202/025-002,
- 750-8202/040-001,
- 750-8203,
- 750-8203/025-000,
- 750-8204,
- 750-8204/025-000,
- 750-8206,
- 750-8206/025-000,
- 750-8206/025-001,
- 750-8207,
- 750-8207/025-000,
- 750-8207/025-001,
- 750-8208, and
- 750-8208/025-000

## ۵. کدهای بهره‌جویی منتشرشده

بر اساس بررسی‌های ما کد بهره‌جویی عمومی برای آسیب‌پذیری CVE-2018-545 وجود ندارد اما این در حالی است که مرجع [۲] ادعا کرده است چنین کد بهره‌جویی وجود دارد؛ اما کدهای بهره‌جویی دیگری برای حمله به نرم‌افزار CoDeSys با آسیب‌پذیری‌های دیگر در جدول ۲ مشخص‌شده است:

**جدول ۲: کدهای بهره‌جویی عمومی منتشرشده نرم‌افزار CoDeSys**

| | | |
|---|---|---|
| **EDB-ID**: 44430 | **Author**: LiquidWorm | **Published**: 2018-04-09 |
| **CVE**: N/A | **Type**: Webapps | **Platform**: Linux |
| **E-DB Verified**: | **Exploit**: Download / View Raw | **Vulnerable App**: N/A |

[1] Firmware

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

| | | |
|---|---|---|
| **EDB-ID**: 41712 | **Author**: Metasploit | **Published**: 2013-02-02 |
| **CVE**: CVE-2012-4705 | **Type**: Local | **Platform**: Windows |
| **Aliases**: N/A | **Advisory/Source**: Link | **Tags**: N/A |
| **E-DB Verified**: ✔ | **Exploit**: Download / View Raw | **Vulnerable App**: N/A |

| | | |
|---|---|---|
| **EDB-ID**: 18240 | **Author**: Metasploit | **Published**: 2011-12-13 |
| **CVE**: CVE-2011-5007 | **Type**: Remote | **Platform**: Windows |
| **Aliases**: N/A | **Advisory/Source**: N/A | **Tags**: Metasploit Framework (MSF) |
| **E-DB Verified**: ✔ | **Exploit**: Download / View Raw | **Vulnerable App**: N/A |

## ۶. تاریخچه آسیب‌پذیری‌های محصولات تحت تأثیر

جدول ۳: برخی آسیب‌پذیری‌های مهم محصولات تحت تأثیر

| | |
|---|---|
| Base Score: 10.0 Critical | CVE-2012-6069 |
| Base Score: 10.0 Critical | CVE-2012-6068 |
| Base Score: 7.5 HIGH | CVE-2017-6025 |
| Base Score: 7.5 HIGH | CVE-2017-6027 |

## ۷. توصیه‌ها و راه‌حل‌های امنیتی

- شرکت Wago این آسیب‌پذیری 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 به‌روزرسانی سفت افزار (متأسفانه از طریق لینک ذیل ما نتوانستیم نسخه به‌روزرسانی سفت افزار را دریافت نمایم، امیدواریم این مسئله به‌این‌علت باشد که ما دسترسی به پورتال این شرکت به‌عنوان مشتری را نداریم. چنانچه شما به شناسه مشتری قادر به دانلود وصله امنیتی شدید لطفاً به ما اطلاع دهید تا این لینک را تائید نماییم):

http://global.wago.com/en/services/downloads/firmware-downloads/index.jsp

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که دسترسی به کنترل‌کننده هدف و سامانه مدیریت و نظارت[1] بر آن را محدود کنند؛ این محدودسازی می‌تواند از طریق دیواره‌های آتش کنترل صنعتی یا لیست سفید انجام شود. در صورت عدم به‌روزرسانی محصولات تحت تأثیر حتماً دسترسی آن‌ها به شبکه عمومی (به‌ویژه اینترنت) را قطع نمایید.
- در صورت عدم نیاز به انتقال برنامه به کنترل‌کننده حتماً درگاه شماره ۲۴۵۵ TCP را توسط WBM مسدود نمایید.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک راهکارهای کنترل دسترسی تنها به کاربران مجاز امکان دسترسی به شبکه صنعتی را بدهند.
- 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[2] کنترل صنعتی استفاده نمایند.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک محصولاتی مانند SIEM کنترل صنعتی و سامانه تشخیص نفوذ صنعتی (IDC) به شکل مستمر کلیه تجهیزات سامانه و ترافیک عبوری را پایش نمایند.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که در صورت محدودیت در پلنت صنعتی و جهت اتخاذ رویکرد کاهش مخاطره، سامانه‌های تحت تاثیر را در یک زیرشبکه[3] ایزوله یا محدوده‌ی امن قرار دهند.
- درصورتی‌که در واحد صنعتی 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 ۱ نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر را مشاهده می‌کنید ما در قالب دوره آموزشی پیشرفته می‌توانیم به شما ارائه نماییم.

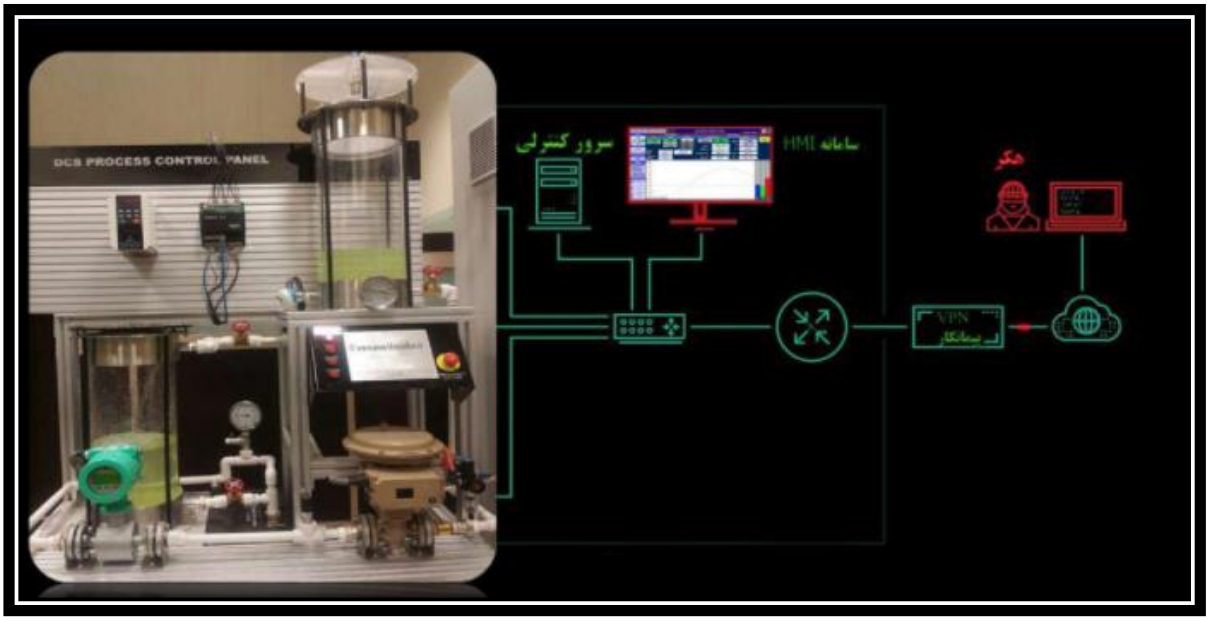
[1] Monitoring

[2] Data Diode

[3] Subnet

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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 ۱: نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر**

- همانند غالب آسیب‌پذیری‌ها و حملات به سامانه‌های 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.)

## ۸. 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 این نمونه می‌بینیم بین زمان تاریخ گزارش آسیب‌پذیری توسط سازنده (7 December 2017) و تاریخ گزارش آسیب‌پذیری توسط ics-cert(14 February 2018) ۶۹ روز فاصله است!

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 (7 December 2017) و ارائه وصله‌ی امنیتی زمان قابل‌توجهی وجود دارد. در

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

مرجع [۲] که به شکل رسمی شرکت WAGO منتشر کرده است می‌بینیم که این شرکت اعلام کرده است که وصله به‌زودی منتشر خواهد شد! (شکل ۲)


**شکل ۲: بخشی از سند رسمی آسیب‌پذیری منتشرشده توسط سازنده [۲]**

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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[1]: 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[2]: 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[3] 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[4] 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:

---

[1] Design/Specification

[2] Implementation

[3] Configuration

[4] Properties

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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 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[۱]، صحت اطلاعات[۲] و دسترس‌پذیری[۳] است که از این سه ویژگی در برخی منابع با عنوان سه‌تایی CIA یاد می‌شود که در شکل ۳ نمایش داده‌شده‌اند. در ادامه این سه ویژگی را تعریف می‌کنیم [۱]:


**شکل ۳: 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<br>• دسترسی غیرمجاز به داده‌ها<br>• سرقت داده‌ها<br>• تعرض به حریم خصوصی |

[1] Confidentiality
[2] Integrity
[3] Availability

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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<br>• جعل داده‌ها |
| **دسترس‌پذیری** | دسترسی به داده‌ها توسط افراد مجاز در هر مکان و در هرزمان | • از دسترس خارج شدن خدمات یک کارگزار<br>• نابودی داده‌ها<br>• 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

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

## 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].

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

# 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 که تمایل دارند نامه یا پیام ارسالی خود را با یک‌لایه امنیتی (رمزنگاری) برای بنده ارسال کنند می‌توانند از کلید عمومی PGP بنده (لینک) برای ارسال رمز شده نامه خود استفاده کنند.

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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

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**

## 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 | | سومین کنفرانس و نمایشگاه فناوری اطلاعات و ارتباطات در | دی ۱۳۹۳ | لینک |

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

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

| | | | | |
|---|---|---|---|---|
| پتروشیمی | | صنایع نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی | | |




بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.

# منابع و مراجع

۱. احمدیان، محمد مهدی؛ رضا زاده، بابک. پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری، انستیتو ایزایران، ۱۳۹۶

2. WAGOWebsite http://global.wago.com/media/2_products/security/Sec-Advisory_CoDeSys.pdf
3. https://ics-cert.us-cert.gov/advisories/ICSA-13-011-01
4. https://ics-cert.us-cert.gov/advisories/ICSA-18-044-01
5. https://tools.cisco.com/security/center/viewAlert.x?alertId=56812
6. https://vuldb.com/?id.113207
7. https://nvd.nist.gov/vuln/detail/CVE-2018-5459
8. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-341-01
9. https://www.sec-consult.com/en/blog/advisories/wago-pfc-200-series-critical-codesysvulnerabilities/index.html
10. https://en.wikipedia.org/wiki/CODESYS
11. https://securityaffairs.co/wordpress/68569/hacking/codesys-ics-flaw.html
12. https://nvd.nist.gov/vuln/detail/CVE-2012-6068
13. https://nvd.nist.gov/vuln/detail/CVE-2012-6069
14.

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

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

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی‌برداری از مطالب این سند، بدون درج نام مؤلف سند، غیرقانونی است و می‌تواند پیگرد قانونی داشته باشد.