安天智甲有效防护 Revon 勒索软件变种

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Revon 的勒索软件变种，该勒索软件隶属于 Phobos 勒索软件家族，最早于 2020 年 4 月被发现，主要通过垃圾邮件传播。安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻止 Revon 勒索软件的加密行为。

Revon 勒索软件执行后，加密计算机上的可执行程序和文档文件，在原文件名后追加名为“.id[USER_ID].[werichbin@protonmail.com].revon”的后缀。该勒索软件加密后创建两种类型的勒索信，一种为 txt 格式，另一种为 hta 格式，勒索信内容包含勒索说明、联系邮箱、比特币购买教程网址和 USER_ID 等。Revon 勒索软件会将自身拷贝到“C:\Users\ 用户名 \AppData\Local”路径下并操作注册表添加表项，将其设置为开机自启动。Revon 勒索软件使用“AES+RSA”加密算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、删除本地计算机的备份目录等。目前被加密的文件在未得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的口令；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、关联分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器、关联分析鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	daeea857831d0d022fbbae530557cb48480ff0370decec3d41d4dbdfc672d3db
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	56 KB
MD5	034711DED900D781E170C660BEC9AB86
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Occamy
判定依据	反病毒引擎

◆ 操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
删除全盘所有卷影副本	★★★★
文件篡改	★★★★★
延时	★★★
检测虚拟机	★★★★★
.....	.....

◆常见行为

行为描述	危险等级
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
打开自身进程文件	★
.....	.....

◆ 完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 4 月 20 日 (总第 227 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

CODESYS V3 未经身份验证的远程堆溢出漏洞分析与复现

概述

2020 年 3 月 25 日 CODESYS 发布 CODESYS V3 未经身份验证的远程堆溢出漏洞，攻击者利用精心设计的请求可能会导致基于堆的缓冲区溢出。CODESYS 软件工具包是一款基于先进的 .NET 架构和 IEC 61131-3 国际编程标准的面向工业 4.0 及物联网应用的软件开发平台。CODESYS 软件平台可实现逻辑控制（PLC）、运动控制（Motion Control）及 CNC 控制、人机界面（HMI）、基于 Web Service 的网络可视化编程和远程监控、冗余控制 (Redundancy) 和安全控制（Safety）、项目开发与工程协同管理等多个目标和需求。

安天针对 CODESYS 的 CVE-2020-10245 漏洞进行了分析和复现，该漏洞存在于 CmpWebServerHandlerV3.dll（文件版本 3.5.15.20）库中，源于该 dll 库未能正确验证由用户提交的发往 Web Server URL 端点的数据。此漏洞会造成 Web 服务器崩溃、拒绝服务或者可能被用于远程代码执行。对此，安天研究人员分析了该漏洞原理并给出相应的防护建议。

漏洞情况

该漏洞允许未经身份验证的远程攻击者破坏服务器或远程代码执行。存在漏洞的服务器用于在 Web 浏览器中显示 CODESYS 系统可视化屏幕。该漏洞基于堆的缓冲区溢出，是由于名为 CmpWebServerHandlerV3.dll 的 Web 服务器库无法正确验证发送到 Web 服务器 URL 端点的用户数据而导致。攻击者可以通过发送给 CmpWebServerHandlerV3 组件的 WEB_CLIENT_OPENCONNECTION 消息请求非常大的内存分配，来利用这个漏洞，最终导致 Web 服务器崩溃、拒绝服务或远程执行代码。该漏洞严重程度评分如下表所示：

	CVSS v2.0	CVSS v3.1
基本得分	10	9.8
向量	AV: N/AC: L/Au: N/C: C/I: C/A: C	AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: H/A: H
影响得分	10	5.9
可利用性得分	10	3.9
严重等级	高	高

▲CVSS 评分

●披露时间

2019 年 12 月 02 日：发现漏洞

2019 年 12 月 11 日：CODESYS 承认漏洞。

2019 年 12 月 11 日：CODESYS 预计在 90 天后进行解释。

2020 年 01 月 28 日：供应商通知他们计划在 3 月中旬发布补丁。

2020 年 03 月 18 日：CODESYS 通知，由于 COVID-19，他们需要将其补丁和咨询推迟几天，计划在三月中旬发布版本 3.5.15.40。

2020 年 03 月 25 日：CODESYS 已发布公告和漏洞修复。

●漏洞影响版本

在用于工程控制系统的自动化软件 CODESYS 的 Web 服务器中存在一个严重漏洞，此漏洞存在 V3.5.15.40 之前的所有版本中，所有包含 Web 服务器 (CmpWebServer 和 CmpWebServerHandler) 的 CODESYS V3 系统运行中都会受到影响，主要包括：

- CODESYS Control for BeagleBone
- CODESYS Control for emPC-A/iMX6
- CODESYS Control for IOT2000
- CODESYS Control for Linux
- CODESYS Control for PLCnext
- CODESYS Control for PFC100
- CODESYS Control for PFC200
- CODESYS Control for Raspberry Pi
- CODESYS Control RTE V3
- CODESYS Control RTE V3 (for Beckhoff CX)
- CODESYS Control Win V3 (also part of the CODESYS Development System setup)
- CODESYS HMI V3
- CODESYS Control V3 Runtime System Toolkit
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit

●漏洞影响范围

CODESYS 是一款工业自动化领域的一款开发编程系统，应用领域涉及工厂自动化、汽车自动化、嵌入式自动化、过程自动化和楼宇自动化等。CODESYS 软件可以分为两个部分，一部分是运行在各类硬件中的 RTE（Runtime Environment），另一部分是运行在 PC 机上的 IDE。因此 CODESYS 的用户既包括生产 PLC、运动控制器的硬件厂商，也包括最终使用 PLC、运动控制器的用户。

目前全球有近 400 家的控制系统生产制造商是 CODESYS 的用户：如 ABB、施耐德电气 SchneiderElectric、伊顿电气 EATON、博世力士乐 Rexroth、倍福 BECKHOFF、科控 KEBA、日立 HITACHI、三菱自动化 MITSUBISHI、欧姆龙 OMRON、研华科技、凌华科技 ADLINK、和利时集团、SUPCON 中控集团、步科自动化 KINCO 等等。

漏洞原理及复现过程

●漏洞原理

攻击者可借助特制的请求，利用该漏洞造成基于堆的缓冲区溢出，攻击者通过与服务端建立连接，并请求分配内存，服务器响应攻击者并分配内存，攻击者发送

（下转第三版）

每周安全事件

类 型	内 容
中文标题	美国棕榈滩县计算机系统遭勒索软件攻击
英文标题	REvil Rocks Jupiter
作者及单位	Sarah Coble
内容概述	3 月 21 日，棕榈滩县 (Palm Beach County) 遭到了 REvil 勒索软件（也称 Sodinokibi) 的攻击，导致该县的计算机系统瘫痪了三周。Jupiter 的公共信息官员 Kate Moretto 证实，该事件导致多个文件被加密。来自网络空间的威胁使得 Jupiter 的员工无法访问其电子邮件帐户来开展城镇业务。居民无法使用在线服务进行公用事业付款，该镇的在线计划提交系统也被关闭。到 4 月 10 日，该镇的大多数数字服务已恢复，该镇的网站再次运行。
链接地址	https://www.infosecurity-magazine.com/news/revil-rocks-jupiter/

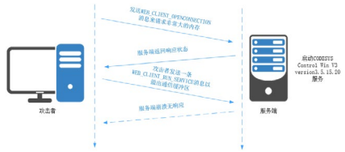
每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.spynote.d[prv,exp,rmt,spy] 2020-04-13	高	该应用程序是间谍软件，运行隐藏图标，诱导激活设备管理器，接收远程指令，上传联系人、通话记录、安装列表、位置、录音文件等隐私，还会接收指令拨打电话，下载未知文件会造成用户隐私泄露和资费损耗，请卸载。
		Trojan/Android.GSpy.hd[prv,spy] 2020-04-14	中	该应用程序包含恶意代码，运行后台会自动启动摄像头录制视频，窃取用户通讯录信息、手机设备固件信息等上传，为避免造成用户隐私泄露，建议卸载。
		G-Ware/Android.FakeSystem.bj[rog,exp] 2020-04-15	低	该应用程序伪装成系统应用，运行会后台频繁访问指定网址，造成用户资费消耗，建议不要使用。
	较为活跃样本	Trojan/Android.ubiporspy.a[prv,exp,rmt,spy]	中	该应用程序是一款间谍应用，程序运行会隐藏图标，请求激活设备管理器，后台窃取 GPS 位置信息、通话录音等隐私信息联网上传，监听短信获取短信指令，通过短信指令远控执行窃取用户 GPS 位置信息、开启环境录音、发送短信等行为，造成用户隐私泄露和资费消耗，建议立即卸载。
		Trojan/Android.Joker2.ak[prv,pay,exp]	中	该应用程序包含恶意代码，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息，造成用户隐私泄露和经济损失，建议卸载。
		Trojan/Android.Cerberus.b[prv,rmt]	中	该应用程序伪装成其他应用，运行后台监听用户的短信、通知栏信息，窃取短信及固件信息联网上传，并私自发送短信，访问未知页面，造成用户的资费消耗和隐私泄露，建议卸载。
		Trojan/Android.GBanker.eq[prv]	中	该应用程序伪装成系统服务，程序运行后隐藏图标，通过虚假界面盗取银行信息，同时窃取用户短信和通讯录上传到远程服务器，还会私发短信，造成用户隐私泄露和财产损失，建议卸载。
		Trojan/Android.Evile8game.a[exp,rog]	低	该应用程序包含恶意代码，运行后联网加载恶意子包，上传用户手机基本信息，推送流氓广告，模拟用户点击进行刷量操作。造成用户流量消耗。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	脚本引擎内存损坏漏洞（CVE-2020-0768）	高	在 Microsoft 浏览器脚本引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	较为活跃样本	Trojan[PSW]/Win32.Papras	中	此威胁是一种恶意的木马类程序。该家族样本运行后自我复制到被感染计算机系统的指定目录下并调用执行。在系统目录下释放一个恶意驱动文件，该文件采用高级 Rootkit 技术编写，隐藏自我，防止被查杀。窃取被感染计算机系统中用户的机密信息并回传，在后台与指定站点交互大量垃圾数据，占用网络资源，影响用户使用。
		Trojan[Spy]/Win32.KeyLogger	中	此威胁是一种间谍类木马程序。该家族样本运行后会监视用户的键盘操作，记录用户的击键记录并上传至远程服务器，以窃取用户敏感信息。
		Trojan/Win32.Conycspa	中	此威胁是一种可以释放其他恶意代码的木马家族。该家族样本运行后可以释放恶意代码并运行，可能会窃取用户信息并回传、连接网络下载其他恶意代码等。
		RiskWare[Downloader]/Win32.Gnome	低	此威胁是一种可以下载推广应用的风险软件家族。该家族样本运行后连接网络下载推广应用并安装，占用系统资源，影响用户使用。
		GrayWare[AdWare]/Win32.PurityScan	低	此威胁是一种可以下载并安装推广应用的灰色软件家族。该家族样本运行后可以连接网络下载并安装推广应用，占用系统资源，影响用户使用。

（上接第一版）

特殊消息使服务端缓冲区溢出，导致 Web Server 发生崩溃。如下图所示：



▲ CODESYS 缓冲区溢出过程

该漏洞存在于 CmpWebServerHandlerV3.dll（文件版本 3.5.15.20）库中，源于该 dll 库未能正确的验证由用户提交的发往 Web Server URL 端点的数据。当 CmpWebServerHandlerV3 组件状态为“0”时，攻击者可通过向 CmpWebServerHandlerV3 组件发送一条 WEB_CLIENT_OPENCONNECTION 消息，请求分配大小为 0xffffffff 的缓冲区，在缓冲区分配操作过程中 SysMemGetCurrentHeapSize 函数被 SysMemAllocData 函数调用向所请求的缓冲区分配大小添加了 0x5c 字节，缓冲区分配大小会溢出，即实际上分配了一块小的堆缓冲区（0xffffffff+ 0x5c = 0x5b）。攻击者通过发送一条精心构造的 WEB_CLIENT_RUN_SERVICE 消息以溢出小型通信缓冲区，造成缓冲区溢出，进而使 Web Server 崩溃。

●复现过程

攻击者通过与服务端建立连接，并请求分配内存，服务器响应攻击者并分配内存，攻击者发送特殊消息使服务端缓冲区溢出，导致 Web 服务器发生崩溃。基于以上漏洞原理，搭建复现环境，通过 POC 脚本对漏洞进行复现。

复现环境采用 CODESYS V3.5.15.20（32 位）版本，Windows10 家庭版，8G 内存，搭建服务端环境。服务端复现环境搭建成功后，结合漏洞原理及 POC 程序针对该漏洞进行了复现。

该 POC 是由 Python 语言实现，在执行过程中需要配置目标地址（Web Server 服务器地址）和目标端口号（默认为 8080）。查看正常状态下 Web Server 服务及 Web 访问状态。Web Server 服务状态如下图所示：

▲ POC 执行前服务状态

被用来测试的 Web 访问页面，可正常访问，如下图所示：

▲ POC 执行前 WEB 访问状态

运行 POC 前重启 CODESYS 服务，使 CmpWebServerHandlerV3 组件处于状态“0”。运行 POC 脚本，连接服务端并请求分配内存。POC 脚本部分代码如下图所示：

```
open_conn = base64.b64encode("\x01\x00\x00\x00" + "|foo|-1|true|")
headers = {"Connection": "keep-alive", "3S-Repl-Content": open_conn}
conn.request("POST", url, "", headers)
res = conn.getresponse()
```

▲ POC 部分代码

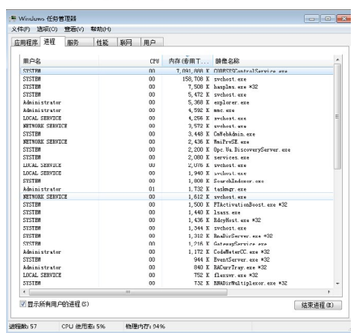
POC 运行后，查看 Web Server 及 Web 访问状态，Web Server 服务已经停止，如下图所示：

▲ POC 执行后服务状态

被用来测试的 Web 页面不能正常访问，重新启动服务后，页面访问恢复正常。不能正常访问时状态如下图所示：

▲ POC 执行后 WEB 访问状态

针对 CODESYS V3.5.15.20（64 位）版本，采用 Windows7（64 位）系统，8G 内存，搭建服务端环境。客户端运行 POC 后，服务端内存被占满，随着时间推迟内存被慢慢释放，Web 服务没有停止，但 Web 页面不能访问，造成拒绝服务攻击。



▲服务端内存使用过高

被用来测试的 Web 页面不能正常访问，服务重启后，Web 页面才可正常访问。Web Server 服务重启后，Web 页面可正常访问。

漏洞危害及防护建议

●漏洞危害

本次复现漏洞可能导致 Web 服务器崩溃、拒绝服务，或者可能被用于远程代码执行。下面对有可能造成的危害进行详细说明：

(1) Web 服务崩溃：CODESYS Web Server 在工业控制系统场景中可用来作为 Web SCADA 服务器，Web SCADA 服务器崩溃可导致与控制器通信中断，不能接收来自控制器返回的数据信息，不能对控制器参数进行修改。可能使工业控制系统发生异常，导致企业停工停产，造成安全威胁或经济损失。

(2) 远程代码执行：攻击者利用该缓冲区溢出漏洞可能导致工业控制系统数据泄露，如软件版本，系统信息、工艺参数等关键数据，为进一步攻击工业控制系统做信息收集准备；也可通过 shell 脚本获取工业控制系统操作权限，对工业控制系统正常运行带来影响。

●防护建议

根据该漏洞的原理及官网针对该漏洞的修复情况，给出以下建议。

(1) 建议将 CODESYS 软件升级到 V3.5.15.40，官方在 V3.5.15.40 版本中修复此漏洞。

(2) 对运行 CODESYS Control Service 的主机配置防火墙限制 IP 访问，仅允许指定 IP 访问，禁止外部 IP 访问，并进行相应的访问日志审计，防止系统信息泄露。

(3) 禁止工业控制网络在无防护设备情况下与互联网连接，如必须连接互联网可采取安装工业防护设备（防火墙、网闸等）来限制攻击者的入侵。

(4) 增加工业网络流量检测和监测设备，对 Web 管理平台异常流量进行阻断、报警、及时发现，防止工业系统敏感信息泄露。

以上内容为精简版
扫描二维码可阅读全文