



Endüstriyel KAOS (SCADA Hacking)

SignalSEC

www.signalsec.com



SignalSEC
get signal before them

Yeni Nesil Silahlar 😊

- Odayler ve komplike zararlı yazılımlar



Ajanda

- Hakkımızda
- SCADA hedefli ataklar
- Açıklar
- Sıfır gün (Zero-day) Açıklar
- Exploitation
- Post-exploitation
- Demo

Hakkımda

- Bilgi Güvenliđi Arařtırmacısı @ SignalSEC
- Reversing , Vulnerability Research ve Exploiting ilgilisi
- Uluslararası “**hacker**” konferanslarında konuřmacı
- Adobe, IBM , Microsoft, Novell, Facebook vb. birok őründe zafiyet avcısı (bug hunter)



Nasıl Başladı?

- 2010 öncesine kadar güvenlik vakası yoktu ?!
- Temmuz 2010 – **Milat** : **STUXNET** Vakası
- Hackerlar ve güvenlikçiler SCADA pastasının tadına vardı 😊 :
 - Internet'e açık binlerce SCADA Sistem
 - Buggy Softwares
 - Popülerite

SONUÇ : Risk artışı !!!!

İnternet'e açık yüzlerce SCADA

- Banner bilgisi ve tarama ile ulaşmak..
- Kısıtlı (?) **SHODAN** ' dan birkaç örnek :
- SCX SCADA:
- Banner bilgisi: “**SCXWebServer**”
- Shodan Sonuçları : **77**

SCXWebServer SHODAN

The screenshot shows a web browser window with the address bar displaying `www.shodanhq.com/search?q="SCXWebServer"`. The page header includes the SHODAN logo and navigation tabs: Home, Search Directory, Data Analytics/ Exports, Developer Center, and Labs. Below the header, there are buttons for '+ Add to Directory' and 'Export Data'. The main content area displays search results for 'SCXWebServer', showing 'Results 1 - 10 of about 80'. A table lists top countries matching the search:

Country	Count
United States	31
Canada	19
Finland	9
Russian Federation	8
Australia	6

Below the table, three search results are visible, each showing an IP address, date added, location, and server details:

- 82.215.198.27**: Added on 13.12.2011, Kotka, Details. Server: **SCXWebServer/6.0**. Content-Type: text/xml, Content-Length: 1198.
- 123.209.59.209**: Added on 11.12.2011, Details. Server: **SCXWebServer/6.0**. Content-Type: text/xml, Content-Length: 1235.
- 213.28.34.191**: Added on 09.12.2011, Details.

On the right side of the page, there is an advertisement box with the text 'Advertise Here' and 'Celebrating 2 years of Shodan'. The Windows taskbar at the bottom shows various application icons and the system clock displaying 23:23 on 21.12.2011.

CoDeSys on SHODAN

- Banner bilgisi ve tarama ile ulaşmak..
- Kısıtlı (?) **SHODAN** ' dan birkaç örnek :
- CoDeSys SCADA: Bir çok scada yazılımında kullanılan bir platform
- Banner bilgisi: “**ENIServer**”
- Shodan Sonuçları : **195**
- Şaşırtıcı kurumlar 😊

CoDeSys on SHODAN

The screenshot shows a web browser window with the address bar containing `www.shodanhq.com/search?q="ENIServer"`. The page title is "SHODAN - Computer Search". The navigation menu includes "Home", "Search Directory", "Data Analytics/ Exports", "Developer Center", and "Labs". There are buttons for "Add to Directory" and "Export Data". The search results are displayed as "Results 1 - 10 of about 195 for 'ENIServer'".

» Top countries matching your search

Russian Federation	89
Ukraine	21
Italy	16
Germany	11
Sweden	6

2.94.61.205
Added on 13.12.2011
Details

HTTP/1.0 403 Forbidden
Cache-Control:no-cache no-store
Content-Length:0
Server:ENIServer

46.203.3.174
Added on 11.12.2011
Details

HTTP/1.0 403 Forbidden
Cache-Control:no-cache no-store
Content-Length:0
Server:ENIServer

188.16.232.111
Added on 11.12.2011
Pervouralsk
Details

HTTP/1.0 403 Forbidden
Cache-Control:no-cache no-store
Content-Length:0
Server:ENIServer

31.181.213.22
Added on 11.12.2011
Details

HTTP/1.0 403 Forbidden
Cache-Control:no-cache no-store
Content-Length:0
Server:ENIServer

Advertise Here

Celebrating 2 years of Shodan

TR 23:04 21.12.2011

Şaşırtıcı Kurumlar

- TeliaSonera – Dünyanın en büyük GSM şirketleri grubu
- Vodafone Portekiz

46.189.227.68

Added on 03.03.2011

Details

68.227.189.46.rev.vodafone.pt

HTTP/1.0 403 Forbidden

Cache-Control: no-cache no-store

Content-Length: 0

Server: **ENIServer**

90.237.128.99

Added on 06.04.2011

 Hindás

Details

host-90-237-128-
99.mobileonline.telia.com

HTTP/1.0 403 Forbidden

Cache-Control: no-cache no-store

Content-Length: 0

Server: **ENIServer**

7-T IGSS SCADA Exploit

- 50 ülkede **28 BİN** kurumda kullanılan **SCADA** yazılımı
- Bugüne (22 Aralık 2011) kadar Zero-day idi 😊
- SignalSEC ve ICS-CERT işbirliği ile koordinasyon ve yama süreci tamamlandı.
- http://www.us-cert.gov/control_systems/pdf/ICSA-11-355-01-7.pdf

7-T IGSS ??

- OSLO Trafik Merkezi , Çek Cumhuriyeti Doğalgaz Dağıtımı , Kuala Lumpur Havalimanı



InduSoft SCADA Exploit

- Bir başka popüler SCADA yazılımı
- Zeroday – henüz yamanmadı
- SignalSEC paketinde mevcut
- Invalid Pointer Write (DoS)

CoDeSys **SCADA** WebServer

- **SignalSEC** tarafından ICS-CERT işbirliği ile yama süreci tamamlandı ve yayınlandı.
- Exploit-db ' de yazdığımız örnek bir exploit kodu mevcut.
- Stack tabanlı bir hafıza taşması
- Uzaktan tetiklenebilir

CoDeSys Zafiyet Analizi

- Unsafe function : vsprintf !!!

The image shows a screenshot of assembly code with several windows and annotations. A red circle highlights the format string "%5" in the assembly instruction `push offset aS_5 ; "%5"`. Another red circle highlights the `call _vsprintf` instruction in the assembly window on the right. Blue arrows point from the `call _vsprintf` instruction to the `offset aS_5 ; "%5"` instruction and to the `push eax` instruction above it. Green arrows point from the `push eax` instruction to the `push ecx` instruction above it, and from the `push ecx` instruction to the `push edx` instruction above it. Cyan arrows point from the `push edx` instruction to the `lea ecx, [ebp+var_100]` instruction above it, and from the `lea ecx, [ebp+var_100]` instruction to the `mov [ebp+var_310], ecx` instruction above it.

```
mov [ebp+wParam], 0
mov [ebp+var_320], 0
lea eax, [ebp+arg_4]
mov [ebp+var_314], eax
push offset aFile_0 ; "File"
mov ecx, [ebp+arg_0]
push ecx ; char *
call _strstr
add esp, 8
test eax, eax
jz .

push offset aRequested ; "requested"
mov eax, [ebp+arg_0]
push eax ; char *
call _strstr
add esp, 8

push offset aS_5 ; "%5"
mov edx, [ebp+arg_0]
push edx ; char *
call _strstr
add esp, 8
test eax, eax

loc_40D2F4:
mov ecx, [ebp+var_314]
push ecx ; va_list
mov edx, [ebp+arg_0]
push edx ; char *
lea eax, [ebp+var_100]
push eax ; char *
call _vsprintf
add esp, 0Ch
lea ecx, [ebp+var_100]
mov [ebp+var_310], ecx
```

CoDeSys Zafiyet Analizi

```
004002DE E8 4DB70000 CALL webserve.00418A30
004002E3 83C4 08 ADD ESP,8
004002E6 85C0 TEST EAX,EAX
004002E8 74 0A JE SHORT webserve.004002F4
004002EA C785 E0FCFFFF 0 MOV DWORD PTR SS:[EBP-320],1
004002F4 8B8D ECFCFFFF MOV ECX,DWORD PTR SS:[EBP-314]
004002FA 51 PUSH ECX
004002FB 8B55 08 MOV EDX,DWORD PTR SS:[EBP+8]
004002FE 52 PUSH EDX
004002FF 8D85 00FFFFFF LEA EAX,DWORD PTR SS:[EBP-100]
00400305 50 PUSH EAX
00400306 E8 15D60000 CALL webserve.0041A920
0040030B 83C4 0C ADD ESP,0C
0040030E 8D8D 00FFFFFF LEA ECX,DWORD PTR SS:[EBP-100]
00400314 8B8D ECFCFFFF MOV ECX,DWORD PTR SS:[EBP-314]
```

BP on vsprintf()

```
EAX 0012EA58
ECX 0012EB64
EDX 0042B830 ASCII "File %s requested ..."
EBX 7FFDF000
ESP 0012E82C
EBP 0012EB58
ESI 80000002
EDI 70A71A29 SHLWAPI.70A71A29
EIP 0040D306 webserve.0040D306
```



BINGO !!!

```
Registers (FPU)
EAX 00000001
ECX 00010101
EDX FFFFFFFF
EBX 7FFDF000
ESP 0012EB60 ASCII "a requested ..."
EBP 61616161
ESI 80000002
EDI 70A71A29 SHLWAPI.70A71A29
EIP 61616161
```

- Instruction Pointer'da direkt kontrol !

HACK LIKE MOVIES ! 😊

(Exploitation)

- **SignalSEC** Exploitleri ile **SCADA Hacking**

“ Selling exploit is like selling a firearm. People can use it to help protect themselves or to hurt others. I sleep fine either way 😊” - Alex McGeorge

Post-Exploitation

- Trojan
- Keylogger
- Rootkit
- SCADA proje dosyalarının enfekte edilip , PLC cihazlarının işlevinin değiştirilmesi vb.
- Emre Tınaztepe, Doğan Kurt gibi arkadaşların işi:)

Teşekkürler..

twitter.com/celilunuver

blog.signalsec.com

