From Unknown Parameter to Root: 
A Story of Unexpected Intrusion Testing Results

Yvan Genuer
Security Researcher

ONAPPSIS
Whoiam

Yvan Genuer

- Security Researcher
- 20 years SAP XP
- 10 years SAP Security
- linkedin.com/in/1ggy

Onapsis

- Business Security Market leaders
- Close to 15 years old
- https://www.onapsis.com
- @onapsis
37% of the Global 2000 use SAP
77% of the world’s transaction revenue
100% of F500 Oil & Gas
The SAP Pentest
The SAP Pentest

› 3 days
The SAP Pentest

› 3 days

› 2 systems
The SAP Pentest

› 3 days
› 2 systems
› RISE with SAP

S/4 HANA Cloud
What is RISE with SAP?

- “A complete offering of ERP software, industry practices, and outcome-driven services for migrating your SAP ERP to the cloud” (1)

- “RISE with SAP can transition your current ERP data and processes to the cloud with less risk and without compromise.” (1)

- Run SAP Applications in the cloud, public or private depending on the SAP Application.

(1) - https://www.sap.com/products/rise.html
<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1128/tcp</td>
<td>open</td>
<td>saphostctrl</td>
</tr>
<tr>
<td>1129/tcp</td>
<td>open</td>
<td>saphostctrls</td>
</tr>
<tr>
<td>3200/tcp</td>
<td>open</td>
<td>tick-port</td>
</tr>
<tr>
<td>3201/tcp</td>
<td>open</td>
<td>cpq-tasksmart</td>
</tr>
<tr>
<td>3300/tcp</td>
<td>open</td>
<td>ceph</td>
</tr>
<tr>
<td>3601/tcp</td>
<td>open</td>
<td>visinet-gui</td>
</tr>
<tr>
<td>3901/tcp</td>
<td>open</td>
<td>nimsh</td>
</tr>
<tr>
<td>4800/tcp</td>
<td>open</td>
<td>iims</td>
</tr>
<tr>
<td>20400/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>40000/tcp</td>
<td>open</td>
<td>safetynetp</td>
</tr>
<tr>
<td>40001/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>40002/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>40080/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>44300/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>44401/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>50013/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>50014/tcp</td>
<td>open</td>
<td>hostagent 00 http</td>
</tr>
<tr>
<td>50113/tcp</td>
<td>open</td>
<td>hostagent 01 http</td>
</tr>
<tr>
<td>50114/tcp</td>
<td>open</td>
<td>hostagent 01 https</td>
</tr>
<tr>
<td>56789/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>59713/tcp</td>
<td>open</td>
<td>hostagent 97 http</td>
</tr>
<tr>
<td>64994/tcp</td>
<td>open</td>
<td>SMDAgent admin</td>
</tr>
</tbody>
</table>
The SAP Pentest

› Default password
› Gateway attack
› Message Server attack
› ICM attack
› IGS attack
› SMDAgent P4 attack
The SAP Pentest

- Default password
- Gateway attack
- Message Server attack
- ICM attack
- IGS attack
- SMDAgent P4 attack
The SAP Pentest

- Default password
- Gateway attack
- Message Server attack
- ICM attack
- IGS attack
- SMDAgent P4 attack
- Host Control Service
The SAP Pentest

- Webservice
- SOAP
- 3 namespaces
- 150+ Webmethods
The SAP Pentest

- Webservice
- SOAP
- 3 namespaces
- 150+ Webmethods
- ~10 anonymous

```
1128/tcp open  saphostctrl  saphostctrl
1129/tcp open  saphostctrls  saphostctrls
3200/tcp open  tick port  dispatcher 00
```
The SAP Pentest

**Expected**

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <urn:GetOsData/>
  </soapenv:Body>
</soapenv:Envelope>
```

**Received**

```
http://sapsystem:1128/SAPOscol.cgi

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <urn:GetOsData/>
  </soapenv:Body>
</soapenv:Envelope>
```

```
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>SOAP-ENV:Server</faultcode>
      <faultstring>Unauthorized: User authentication required</faultstring>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
The SAP Pentest

**Expected**

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"

<soapenv:Body>
  <urn:GetOsData/>
</soapenv:Body>
</soapenv:Envelope>
```

**Received**

```

<SOAP-ENV:Body>
  <urn:GetOsData/>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
 xmlns:SAPOscol="urn:SAPo:oscol:1.0"
 xmlns:COLL="urn:SAPo:coll:2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SAPOscol:GetVersionResponse>
      <Version>COLL 22.11 722 - v2.49, AMD/Intel x86_64 with Linux</Version>
    </SAPOscol:GetVersionResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
The SAP Pentest

<?xml version="1.0" encoding="UTF-8"?>
  <SOAP-ENV:Body>
    <SAPHostControl:GetHwConTextResponse>
      <name>user/sap/tmp/hwconfig</name>
      <content><![CDATA[LINUX Configuration for server]]></content>
      <generated>Tue Jun 20 00:38:52 2023</generated>
    </SAPHostControl:GetHwConTextResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
The SAP Pentest

.............

.............

.............

<urn:GetHwConfText/>

<soapenv:Body>

 Linux version 3.10.0-957.5.1.el7.x86_64 (mockbuild@86-019.build.eng.bos.redhat.com) [gcc version 4.8.5 20150623 (Red Hat (®) 4.8.5-2)]

 response time: 7607ms (1866143 bytes)

</SAPHostControl:ListInstancesResponse>
Remote SAP Host Control configuration

```xml
<soapenv:Envelope xmlns:soapenv=""/>
  <soapenv:Header/>
  <soapenv:Body>
    <urn:GetHWConfText/>
  </soapenv:Body>
</soapenv:Envelope>

SAP Host Agent

/usr/sap/hostctl/exe/host_profile:
SAPSYSTEMNAME = SAP
SAPSYSTEM = 99
DIR_LIBRARY = /usr/sap/hostctl/exe
DIR_EXECUTABLE = /usr/sap/hostctl/exe
DIR_PROFILE = /usr/sap/hostctl/exe
DIR_GLOBAL = /usr/sap/hostctl/exe
DIR_INSTANCE = /usr/sap/hostctl/exe
DIR_HOME = /usr/sap/hostctl/work
service/porttypes = SAPHostControl SAPOscol SAPCCMS
service/admin_users = dadaadm
service/trace = 2
hostexec/trace = 2
service/localconnection = compat
/usr/sap/hostctl/work/dev_saphostexec:

trc file: "dev_saphostexec", trc level: 2, release: "722"
Remote SAP Host Control configuration

```
<soapenv:Envelope xmlns:soapenv=""
    xmlns:soapenv:Header/>
    <soapenv:Body>
        <urn:GetHwConfText/>
    </soapenv:Body>
</soapenv:Envelope>

SAP Host Agent

/usr/sap/hostctrl/exe/host_profile:
SAPSYSNAME = SAP
SAPSYS = 99
DIR_LIBRARY = /usr/sap/hostctrl/exe
DIR_EXECUTABLE = /usr/sap/hostctrl/exe
DIR_PROFILE = /usr/sap/hostctrl/exe
DIR_GLOBAL = /usr/sap/hostctrl/exe
DIR_INSTANCE = /usr/sap/hostctrl/exe
DIR_HOME = /usr/sap/hostctrl/work
service/porttypes = SAPHostControl SAPOscol SAPCCMS
service/admin_users = daaadm
service/trace = 2
```

```
/service/localconnection = compat
```

```
/usr/sap/hostctrl/work/dev_saphostexec:

---
trc file: "dev_saphostexec", trc level: 2, release: "722"
```
32 additionally webmethods exposed
Some of them without authentication
The SAP Pentest

- 32 additionally webmethods exposed
- Some of them without authentication

<table>
<thead>
<tr>
<th>SAPOscol</th>
<th>SAPHostControl</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetVersion</td>
<td>ListInstances</td>
</tr>
<tr>
<td>GetOsData</td>
<td>ListDatabaseSystems</td>
</tr>
<tr>
<td>SendRequestAsync</td>
<td>ListDatabases</td>
</tr>
<tr>
<td>SendRequest</td>
<td>GetComputerSystem</td>
</tr>
<tr>
<td>GetHwConfXML</td>
<td>ExecuteOutsideDiscovery</td>
</tr>
<tr>
<td>GetHwConfText</td>
<td>ConfigureOutsideDiscovery</td>
</tr>
</tbody>
</table>
The SAP Pentest

The Unknown Parameter
The Unknown Parameter

- End of execution phase
- Start writing the report
- Look for parameter information
The Unknown Parameter

Curiosity ++
The Unknown Parameter

Report a security issue

SAP is committed to identifying and addressing security issues that affect our software solutions. We are continuously working on improving our security processes. To report a security issue, choose from the options below.

**SAP customers**
Report a customer security issue to find a solution and get real-time support from an expert.

View the launchpad ›

**Security researchers**
Inform the SAP Product Security Response Team of a security issue by completing and submitting the security vulnerability form.

Access the form ›

**Suppliers**
Inform SAP of a security issue.
The Unknown Parameter

Report a security issue

SAP is committed to identifying and addressing security issues that affect our software solutions. We are continuously working on improving our security processes. To report a security issue, you can use the following resources:

**SAP customers**
Report a customer security issue to find a solution and get real-time support from an expert.

[View the launchpad →](#)

**Security researchers**
Inform the SAP Product Security Response Team of a security issue by completing and submitting the security vulnerability form.

[Access the form →](#)

**Suppliers**
Inform SAP of any security issues discovered in our products.

[Access →](#)

Curiosity +++
The SAP Pentest

The Unknown Parameter

Vulnerability Research
Vulnerability Research

Netweaver JAVA  S/4 HANA  Netweaver ABAP
Accomplish several life-cycle tasks

OS independent

Part of SAP system
Vulnerability Research

Netweaver JAVA

S/4 HANA

Netweaver ABAP

[user@saphost ~]# ps -ef | grep hostctrl
root  42100  1  0 Jun13  ?   00:00:16 /exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile
root  42241  1  0 Jun13  ?   00:02:15 /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile
sapadm 42110  1  0 Jun13  ?   00:01:56 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D

[user@saphost ~]# ss -la|grep 421
LISTEN    0      20      *:1128      *:*                   users:($("sapstartsrv",pid=42110,fid=18))
ESTAB  0      0  saphost:1128  saphost:47510
ESTAB  0      0  saphost:1128  saphost:47514
users:($("sapstartsrv",pid=42110,fid=24))
users:($("sapstartsrv",pid=42110,fid=26))
Vulnerability Research

Netweaver JAVA

S/4 HANA

Netweaver ABAP

[user@saphost ~]# ps -ef | grep hostctrl
root  42100  1  0 Jun13 ?    00:00:16
root  42241  1  0 Jun13 ?    00:02:15
sapadm 42110  1  0 Jun13 ?    00:01:56

[user@saphost ~]# ss -t
LISTEN  0  20        0.0.0.0:1128 SAP Host Ctrl
        0            0 saphost:1128
        0            0 saphost:47514

./exe/saphostexec -start pf=/usr/sap/hostctrl/exe/saposcol -l

/usr/sap/hostctrl/exe/sapstartsrv

users:(["sapstartsrv",pid=42110,fd=18])
users:(["sapstartsrv",pid=42110,fd=24])
users:(["sapstartsrv",pid=42110,fd=26])
Vulnerability Research

Netweaver JAVA

S/4 HANA

Netweaver ABAP

[ user@saphost]

root 4210

root 4224

sapadm 4211

00:00:16 /exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile
00:02:15 /usr/sap/hostctrl/exe/saposcol -1 -w60 pf=/usr/sap/hostctrl/exe/host_profile
00:01:56 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D

users:(["sapstartsrv",pid=42110,fd=18])
users:(["sapstartsrv",pid=42110,fd=24])
users:(["sapstartsrv",pid=42110,fd=26])
Vulnerability Research

Netweaver JAVA

S/4 HANA

Netweaver ABAP

[user@saphost ~]# ps -ef | grep hostctrl
root  42100  1  0 Jun13 ?  00:00:16 ./exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile
root  42241  1  0 Jun13 ?  00:02:15 /usr/sap/hostctrl/exe/saposcol -w60 pf=/usr/sap/hostctrl/exe/host_profile
smpadm 42110  1  0 Jun13 ?  00:01:56 /usr/sap/hostctrl/exe/sapstarcry pf=/usr/sap/hostctrl/exe/host_profile -D

[user@saphost ~]# ss -tanhtp | grep 421
LISTEN  0  20 *:1128
ESTAB  0  0 saphost:1128
ESTAB  0  0 saphost:1128
<table>
<thead>
<tr>
<th>SAPOscol</th>
<th>SAPHostControl</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetVersion</td>
<td>ListInstances</td>
</tr>
<tr>
<td>GetOsData</td>
<td>ListDatabaseSystems</td>
</tr>
<tr>
<td>SendRequestAsync</td>
<td>ListDatabases</td>
</tr>
<tr>
<td>SendRequest</td>
<td>GetComputerSystem</td>
</tr>
<tr>
<td>GetHwConfXML</td>
<td>ExecuteOutsideDiscovery</td>
</tr>
<tr>
<td>GetHwConfText</td>
<td>ConfigureOutsideDiscovery</td>
</tr>
<tr>
<td>SAP Oscol</td>
<td>SAP HostControl</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td>GetVersion</td>
<td>ListInstances</td>
</tr>
<tr>
<td>GetOsData</td>
<td>ListDatabaseSystems</td>
</tr>
<tr>
<td>SendRequestAsync</td>
<td>ListDatabases</td>
</tr>
<tr>
<td><strong>SendRequest</strong></td>
<td>GetComputerSystem</td>
</tr>
<tr>
<td>GetHwConfXML</td>
<td>ExecuteOutsideDiscovery</td>
</tr>
<tr>
<td>GetHwConfText</td>
<td>ConfigureOutsideDiscovery</td>
</tr>
<tr>
<td>Request</td>
<td>Payload</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>99</td>
<td>97</td>
</tr>
<tr>
<td>100</td>
<td>98</td>
</tr>
<tr>
<td>101</td>
<td>99</td>
</tr>
<tr>
<td>102</td>
<td>100</td>
</tr>
<tr>
<td>103</td>
<td>101</td>
</tr>
<tr>
<td>104</td>
<td>102</td>
</tr>
<tr>
<td>105</td>
<td>103</td>
</tr>
<tr>
<td>106</td>
<td>104</td>
</tr>
<tr>
<td>107</td>
<td>105</td>
</tr>
<tr>
<td>108</td>
<td>106</td>
</tr>
<tr>
<td>109</td>
<td>107</td>
</tr>
<tr>
<td>110</td>
<td>108</td>
</tr>
<tr>
<td>111</td>
<td>109</td>
</tr>
<tr>
<td>Request</td>
<td>Payload</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>99</td>
<td>97</td>
</tr>
<tr>
<td>100</td>
<td>98</td>
</tr>
<tr>
<td>101</td>
<td>99</td>
</tr>
<tr>
<td>102</td>
<td>100</td>
</tr>
<tr>
<td>103</td>
<td>101</td>
</tr>
<tr>
<td>104</td>
<td>102</td>
</tr>
<tr>
<td>105</td>
<td>103</td>
</tr>
<tr>
<td>106</td>
<td>104</td>
</tr>
<tr>
<td>107</td>
<td>105</td>
</tr>
<tr>
<td>108</td>
<td>106</td>
</tr>
<tr>
<td>109</td>
<td>107</td>
</tr>
<tr>
<td>110</td>
<td>108</td>
</tr>
<tr>
<td>111</td>
<td>109</td>
</tr>
</tbody>
</table>

```xml
<SOAP-ENV:Header>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
  <SAPoscol:SendRequestResponse>
    <Result>
      06#xA;Wed Jun 21 06:18:10 2023#xA;&#xA;&#xA;&#xA;#
    </Result>
    <rtc>
      0
    </rtc>
  </SAPoscol:SendRequestResponse>
</SOAP-ENV:Body>
```

<urn:SAPMetricService xmlns:SAPMetricService="urn:SAPMetricService" xmlns:SAPoscol="urn:SAPoscol">
[user@saphost ~]# ps -ef | grep hostctrl
root  42100  1  0 Jun13 ?    00:00:16 /exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile
root  42241  1  0 Jun13 ?    00:02:15 /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile
sadm  42110  1  0 Jun13 ?    00:01:56 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D

[user@saphost ~]# ss -larpnt | grep 421
LISTEN  0  20    *:1128    *:*               users:({"sapstartsrv","pid=42110","fd=18"})
ESTAB   0  0    saphost:1128 saphost:47510 users:({"sapstartsrv","pid=42110","fd=24"})
ESTAB   0  0    saphost:1128 saphost:47514 users:({"sapstartsrv","pid=42110","fd=26"})
Vulnerability Research

```
./exe/saphostexec -start pi=/usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/
```

```
ESTAB 0 0  saphost:1128  saphost:47510  users:({"sapstartsrv",pid=42110,fd=24})
ESTAB 0 0  saphost:1128  saphost:47514  users:({"sapstartsrv",pid=42110,fd=26})
```
Vulnerability Research

[user@saphost exe]# /usr/sap/hostctrl/exe/saposcol -h

Saposcol Usage:

* start Saposcol:
  * ./saposcol [-l] [pf=complete name of saposcol profile]

* stop Saposcol:
  * ./saposcol -k [pf=complete name of saposcol profile]

* show Saposcol Status:
  * ./saposcol -s [pf=complete name of saposcol profile]

* call Saposcol dialog interface:
  * ./saposcol -d [pf=complete name of saposcol profile]
Vulnerability Research

[user@saphost exe]# /usr.sap/hostctrl/exe/saposcol -h

*********************************************************************************
* Saposcol Usage:
*
* start Saposcol:
* ./saposcol [-l] [pf=complete name of saposcol profile]
* stop Saposcol:
* ./saposcol -k [pf=complete name of saposcol profile]
* show Saposcol Status:
* ./saposcol -s [pf=complete name of saposcol profile]
* call Saposcol dialog interface:
* ./saposcol -d [pf=complete name of saposcol profile]
*
Vulnerability Research

```
[user@saphost exe]# ./saposcol -d
******************************************************************************
* This is Saposcol Version COLL 22.11
* Please use 'help' to see the usage.
******************************************************************************
Collector >
Collector > ask
ask
Please enter one of
   TestCom  <text>
   DirFree  <path>
   DirInfo  <path>
   RawFree  <path>
   CollTime 
   CollZoneTime
   Path
   NetColl
   MemUse   <PID>
   TraceTyp <Bereich>
   OsSysLog <numbers of lines>
   OsSpecial
   TraceValues
   Hardware
   HardwareXML
Collector >
```
Vulnerability Research

[Unix prompt]

```
user@feasphost exe]# ./saposcol -d
* This is Saposcol Version COLL 22.11
* Please use 'help' to see the usage.

Collector >
Collector > ask CollTime
ask CollTime
Please enter one of
   TestCom <text>
   DirFree <path>
   DirInfo <path>
RawFree <path>
CollTime
CollZoneTime
MemUse <PID>
TraceTyp <Bereich>
OsSysLog <numbers of lines>
OsSpecial
TraceValues
Hardware
HardwareXML
Collector >
```

```python
Collector > ask CollTime
ask CollTime
Wait for exclusive access to shared memory
Sending request with parameter[].
== request send.
looking for answer..
looking for answer..
========= Received =========
Block=[0
Wed Jun 21 06:22:23 2023
]
== results in ==========
Rc=0
P1=Wed Jun 21 06:22:23 2023
P2=
P3=
==========
Collector >
```
102 = “ask CollTime”
Vulnerability Research

```
[user@saphost exe]# ./saposcol -d
******************************************************************************
* This is Saposcol Version COLL 22.11
* Please use 'help' to see the usage.
******************************************************************************
Collector >
Collector > ask
ask
Please enter one of:
    TestCom <text>
    DirFree <path>
    DirInfo <path>
    RawFree <path>
    CollTime
    CollZoneTime
    Path
    NetColl
    MemUse <PID>
    TraceTyp <Bereich>
    OsSysLog <numbers of lines>
    OsSpecial
    TraceValues
    Hardware
    HardwareXML
```

Testing all of them
Testing all of them
Image content includes a code snippet and a vulnerability research context.

Code snippet:
```assembly
0x416a46 <DoRequests+822>:  pop  r14
0x416a48 <DoRequests+824>:  pop  r15
0x416a4a <DoRequests+826>:  leave
0x416a4b <DoRequests+827>:  ret
0x416a4c <DoRequests+828>:  cmp  ebx,0x68
0x416a4f <DoRequests+831>:  je   0x417408 <DoRe...
```

Legend:
- **code**: code segment
- **data**: data segment
- **rodata**: read-only data segment
- **value**: value segment

Stopped reason:
- **SIGSEGV**
- Address: 0x000000000000416a4b in DoRequests ()
checksec /usr/sap/hostctrl/exe/saposcol

[*] '/usr/sap/hostctrl/exe/saposcol'
Arch:       amd64-64-little
RELRO:      No RELRO
Stack:      No canary found
NX:         NX enabled
PIE:        No PIE (0x400000)

Stopped reason: SIGSEGV 0x000000000000416a4b in DoRequests ()
root@system# cat /proc/*/stat
Current RIP addr for saposcol.exe
0x7ffd64b2bee8
### Vulnerability Research

**Current RIP addr for saposcol.exe**

<table>
<thead>
<tr>
<th>Process</th>
<th>State</th>
<th>Address</th>
<th>Args</th>
<th>Line Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>SapoStart</td>
<td>S</td>
<td>54056</td>
<td>54056</td>
<td>-1 1077944384 3579650 5461 0 0</td>
</tr>
<tr>
<td>SapoStart</td>
<td>S</td>
<td>54056</td>
<td>54056</td>
<td>-1 1077944840 3579650 5461 0 0</td>
</tr>
<tr>
<td>SapoStart</td>
<td>S</td>
<td>54056</td>
<td>54056</td>
<td>-1 1077944384 3579650 5461 0 0</td>
</tr>
<tr>
<td>SapoStart</td>
<td>S</td>
<td>54056</td>
<td>54056</td>
<td>-1 1077944840 3579650 5461 0 0</td>
</tr>
</tbody>
</table>

#### EFLAGS: 0x246
- **PARITY**
- **adjust**
- **ZERO**
- **sign**
- **trap**
- **INTERRUPT**

```assembly
    code
    0x7fc29b3fee07 <nanosleep+7>: jne 0x7fc29b3fee19 <nanosleep+
    0x7fc29b3fee09 __nanosleep_nocancel>: mov eax,0x23
    0x7fc29b3fee0e __nanosleep_nocancel+5>: syscall
    0x7fc29b3fee10 __nanosleep_nocancel+7>: cmp rax,0xffffffffffffff
    0x7fc29b3fee16 __nanosleep_nocancel+13>: jae 0x7fc29b3fee49 <n
    0x7fc29b3fee18 __nanosleep_nocancel+15>: ret
    0x7fc29b3fee19 <nanosleep+25>: sub rsp,0x8
    0x7fc29b3fee1d <nanosleep+29>: call 0x7fc29b445bd0 __libc_ena
```

---

**Stack:**

```
0x7f800000 <sleep+212>: mov eax, ebx
```
WE HAVE A LEAK
Skipped .... running quick analysis

Relevant for Non-Unicode systems only,
glibc and saplocales - saplocales must be (re)installed _after_ glibc
RPM-Package: glibc-2.17-260.el7_6.3 Installtime: Mon Feb 1 11:24
RPM-Package: glibc-2.17-260.el7_6.3 Installtime: Mon Feb 1 13:05
package saplocales is not installed
package sap-locale is not installed
package compat-locale-sap is not installed
package compat-locale-sap-common is not installed

glibc and pthread versions:
glibc 2.17
NPTL 2.17

SAPOSCOL data:
******************************************************************************
* This is Saposcol Version COL 22.11.722 - x2 50  _MD(Intel x86)
Skipped .... running quick analysis

Relevant for Non-Unicode systems only,
glibc and gssdp versions: glibc 2.17-260.el7_6.3
RPM-Package: glibc-2.17-260.el7_6.3 Installtime: Mon Feb 1 11:24
RPM-Package: glibc-2.17-260.el7_6.3 Installtime: Mon Feb 1 13:05
package sap-locale is not installed
package compat-locales-sap is not installed
package compat-locales-sap-common is not installed

glibc and pthread versions:
glibc 2.17
NPTL 2.17

SAPOSCOL data:
***********************************************************************
* This is Saposcol Version COLI 22.11.722 - v2.50 AMD(Intel x86)
SSN 3275727 CVE-2023-27498
<table>
<thead>
<tr>
<th>SAPOscol</th>
<th>SAPHostControl</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetVersion</td>
<td>ListInstances</td>
</tr>
<tr>
<td>GetOsData</td>
<td>ListDatabaseSystems</td>
</tr>
<tr>
<td>SendRequestAsync</td>
<td>ListDatabases</td>
</tr>
<tr>
<td>SendRequest</td>
<td>GetComputerSystem</td>
</tr>
<tr>
<td>GetHwConfXML</td>
<td>ExecuteOutsideDiscovery</td>
</tr>
<tr>
<td>GetHwConfText</td>
<td>ConfigureOutsideDiscovery</td>
</tr>
<tr>
<td>SAPOscol</td>
<td>SAPHostControl</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>getVersion</td>
<td>ListInstances</td>
</tr>
<tr>
<td>getOsData</td>
<td>ListDatabaseSystems</td>
</tr>
<tr>
<td>sendRequestAsync</td>
<td>ListDatabases</td>
</tr>
<tr>
<td>sendRequest</td>
<td>GetComputerSystem</td>
</tr>
<tr>
<td>getHwConfXML</td>
<td>ExecuteOutsideDiscovery</td>
</tr>
<tr>
<td>getHwConfText</td>
<td><strong>ConfigureOutsideDiscovery</strong></td>
</tr>
</tbody>
</table>
[user@saphost exe]# ./saphostctrl
Usage: saphostctrl [generic option]... -function <Webmethod> [argument]...
saphostctrl -help [<Webmethod>]

Vulnerability Research
Vulnerability Research

[\texttt{user@saphost.exe}# ./saphostctrl]
Usage: saphostctrl [generic option]... -function <Webmethod> [argument]...
saphostctrl -help [<Webmethod>]

Supported Webmethods:
- ConfigureOutsideDiscovery
  Configure the Outside Discovery Job which runs periodically.
  These Options control the Outside Discovery Job.
  If frequency is not provided, it will run every 12 hours.
  If execution options are not provided the default will be used.
- enable
  \[-frequency <X> \quad \text{Run frequency in minutes}\]
  \[-jobtimeout <X> \quad \text{Wait X seconds for the Outside}\]
[user@saphost exe]# ./saphostctrl -prot tcp -function ConfigureOutsideDiscovery \
-enable \n-sldhost 127.0.0.1 -sldport 1234 \n-sldusername BBBB -sldpassword CCCC

*****************************************************************************
*****************************************************************************
ComputerSystem , string , Enabled
Databases , string , Enabled
[user@saphost exe]# ./saphostctrl -prot tcp -function ConfigureOutsideDiscovery \
  -enable \
  -sldhost 127.0.0.1 -sldport 1234 \n  -sldusername BBBBB -sldpassword CCCCC

*****************************************************************

ComputerSystem , string , Enabled
Databases , string , Enabled

ExecutionFrequencyMinutes , uint64 , 720

*****************************************************************

CreationClassName , string , OutsideDiscoveryDestinations
127.0.0.1_1234 , string , /usr/sap/hostctrl/exe/config.d/slddest_127.0.0.1_1234.cfg
Vulnerability Research

dev_saphostexec log file

[Thr 140090052593664] Current environment will be used
[Thr 140090052593664] Environment:
[Thr 140090052593664] XDG_SESSION_ID=18956
[Thr 140090052593664] HOSTNAME=saphost
[Thr 140090052593664] SHELL=/bin/bash
[Thr 140090052593664] TERM=vt100
[Thr 140090052593664] HISTSIZE=1000
[Thr 140090052593664] USER=root
[Thr 140090052593664] MAIL=/var/spool/mail/root
[Thr 140090052593664] PATH=/usr/bin:/bin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:/root/bin:
[Thr 140090052593664] PWD=/root
[Thr 140090052593664] LANG=en_US.UTF-8
[Thr 140090052593664] HISTCONTROL=ignoredups
[Thr 140090052593664] SHLVL=1
[Thr 140090052593664] HOME=/root
[Thr 140090052593664] LOGNAME=root
[Thr 140090052593664] LESSOPEN=|/usr/bin/lesspipe.sh %s
[Thr 140090052593664] XDG_RUNTIME_DIR=/run/user/0
[Thr 140090052593664] _=/bin/env
[Thr 140090052593664] LD_LIBRARY_PATH=/usr/sap/hostctl/exe
[Thr 140090052593664] PID 117869: root: Executing command "mv -f /usr/sap/hostctl/work/tmpslddest.cfg /usr/sap/config/slddest_127.0.0.1_1234.cfg"
[Thr 140090052593664] CommunicationHeader::Send
dev_saphostexec log file

Executing command "mv -f /usr/sap/hostctrl/work/tmprodssd..."
tcpdump -i lo -A -vv port 1128 or port 1129
tcpdump -i lo -A -vv port 1128 or port 1129

localhost:55011 > localhost.saphostctrl: Flags [P.], cksum 0x02b6 (inco 955100 ecr 1627955100), length 1165
E.....@...f............h.q.Q. ......V.......a....a....POST / HTTP/1.1
Host: localhost:1128
User-Agent: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 1000
Connection: keep-alive
SOAPAction: ""

<SOAP-ENV:Body>
<SAPHostControl:ConfigureOutsideDiscovery>
<configuration>
<flags/>
<status>0D-CFG-ENABLED</status>
<frequency>720</frequency>
<destinations>
<item>
<name>127.0.0.1:1234</name>
<host>127.0.0.1</host>
<port>1234</port>
</item>
</destinations>
<arguments/>
</configuration>
</SAPHostControl:ConfigureOutsideDiscovery></SOAP-ENV:Body>
Vulnerability Research

tcpdump -i lo -A -vv port 1128 or port 1129

```
localhost:55011 > localhost.sahostctrl: Flags [P.], cksum 0x02b6 (inco
a...a...POST / HTTP/1.1
Host: localhost:1128
User-Agent: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 1000
Connection: keep-alive
SOAPAction: ""

<destinations>
  <item>
    <name>127.0.0.1_1234</name>
    <host>127.0.0.1</host>
    <port>1234</port>
    <username>BBBBB</username>
    <password>CCCCC</password>
    <useSSL>false</useSSL>
    <properties></properties>
  </item>
</destinations>
```

No authentication

New parameters in game
SSN 3285757 CVE-2023-24523
The SAP Pentest

The Unknown Parameter

Vulnerability Research

Recommendation
Recommendation

› 3285757 - [CVE-2023-24523] Privilege Escalation vulnerability in SAP Host Agent (Start Service)

› 3275727 - [CVE-2023-27498] Memory Corruption vulnerability in SAPOSCOL

› 3330927 - SAP Host Agent 7.22 PL61 "service/localconnection=compat" removed

› Avoid exposing the SAP Start Service (1128/1129)
The SAP Pentest

The Unknown Parameter

Vulnerability Research

Recommendation

Lessons learned
Lessons learned

» Security by obscurity is not security and it does not work...
Lessons learned

› Security by obscurity is not security and it does not work...

› Security should not be taken for granted
Lessons learned

› Security by obscurity is not security and it does not work...

› Security should not be taken for granted

On premise

In the cloud

Trust But Verify
Lessons learned

› Security by obscurity is not security and it does not work...

› Security should not be taken for granted

› Relationship and partnership respect is crucial in our work
Lessons learned

› Security by obscurity is not security and it does not work...

› Security should not be taken for granted

› Relationship and partnership respect is crucial in our work

› “Breaking is easier than protecting”
Lessons learned

› Security by obscurity is not security and it does not work...

› Security should not be taken for granted

› Relationship and partnership respect is crucial in our work

› “Breaking is easier than protecting”
  → Let's acknowledge the hard work of defenders
THANK YOU!

Yvan Genuer
linkedin.com/in/1ggy
https://www.onapsis.com

ONAPSIS