Project Name: Vulnerability Assessment Big Daddy

# Host Based Information Security Vulnerability Assessment of the Big Daddy Product

*Prepared By Charles Smith 22nd January 2002*

**Document Review**

| **Name** | **Role** | **Review Date** |
|---|---|---|
| Charles Smith | Project Manager | 1/22/2002 |
| Shaun White | Manager (Security) | 1/23/2002 |
| Larry Coryell | Project Manager Big Daddy | |

**References:** See References

**Distribution:** See Distribution

Sun Microsystems, Inc

Cobalt Server Appliance Business Unit

1160 Dublin Road

# 1 Modification Log

| Author | Version | Date | Comment |
|---|---|---|---|
| Charles Smith | 1.0 | 1/22/2002 | Release |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Table of Contents

## 2 Purpose

To provide management part 2 of the three-part Big Daddy Vulnerability Assessment (VA) project, a Host based VA assessment, conducted by the VA Team, Columbus Security Engineering Group.

For purposes of this report, a Host based VA assessment is a point-in-time examination, from an internal operating system viewpoint, i.e. what risks are there from someone on the Internet or Internal gaining unauthorized access to the system by way of vulnerable operating system services and functionalities.

The assessment criteria used to compile this baseline was derived from the identification of known Host level threats and an analysis of the impact of the identified threats against the Big Daddy appliance in it's production configuration, Build 1.49, as it relates to the following three critical business areas of consideration:

- confidentiality - the need to keep proprietary, sensitive, or personal customer information private and inaccessible to anyone who is not authorized to see it

- integrity - the authenticity, accuracy, and completeness of a customer's assets.

- availability - when or how often the customer's asset must be present or ready for use.

## 3 Executive Summary

This report summarizes the Big Daddy Appliance's susceptibility to attack in relation to its Host vulnerabilities. Specifically, the summary graphics describe the severity of vulnerabilities by the percentage and the number found. Vulnerabilities are classified as high, medium, or low. High risk vulnerabilities provide unauthorized, privileged access to the Host, and possibly, the network. Medium risk vulnerabilities provide access to sensitive Host data that may lead to the exploration of higher risk vulnerabilities. Low risk vulnerabilities provide access to sensitive, yet non-lethal, Host data. Appendix A provides a summary of the Vulnerabilities by severity and Appendix B provides a technical breakdown of all of the identified vulnerabilities, coupled with suggested methods for mitigation. Note: The "Check Name" is a vendor-supplied term used for classification purposes only. Please read the description and consequences to have a complete understanding of the issue identified.

# 4 Appendix A – Abbreviated Table of Issues by Risk Level Summary

| Risk Level | Description |
|---|---|
| High | File with insecure permissions has setuid bit set and also has either group or other write permissions set. |
| High | Target file(s) for symbolic links do not exist. |
| High | Files have unusual names |
| Medium | Files have “world” write permissions |
| Medium | Files have “group” write permissions |
| Medium | Files do not match directory owner |
| Medium | Binary files have the setgid bit set |
| Medium | Script files have the setgid bit set |
| Medium | Binary files have the setuid bit set |

# 5 Appendix B – Full Discussion of Issues

**Risk Level**

High

## 5.1 Check Name file_all_04

**Description**

File with insecure permissions has setuid bit set and also has either group or other write permissions set.

**Consequences**

A file that has its setuid bit set and can be written to by group or other is potentially a "Trojan Horse". An unauthorized user could overwrite the file with a different executable (say a shell interpreter), and thus become able to run with the permissions of the owning uid.

**Remedy**

Group write privileges should be removed from the file in question. An attacker gaining root group could truncate and replace the /usr/lib/authenticate binary with arbitrary content, including a shell. This in combination with a vulnerability that allows a local user to get root group would compromise the machine.

**Vulnerability Detail**

| Filename | Perms |
|---|---|
| /usr/lib/authenticate | rwsrwxr-x |

## 5.2 Check Name file-all-08

**Description**

The target files for several symbolic links do not exist.

**Consequences**

When a target file does not exist, this can allow the creation of the target file by an unauthorized user. Additionally, programs that require the file could malfunction or terminate abnormally.

**Remedy**

Remove all symbolic links that do not point to existing files using the rm command, or retrieve the file from a secure backup.

**Vulnerability Detail**

**Filenames**

/etc/rc.d/rcN.d/K07networker

Target path is ../init.d/networker

/etc/rc.d/rcN.d/K09xntpd

Target path is ../init.d/xntpd

/etc/rc.d/rcN.d/K15dhcpd

Target path is ../init.d/dhcpd

/usr/bin/kbdrate

Target path is consolehelper

/usr/lib/groff/tmac/tmac.gmse

Target path is tmac.mse

/usr/man/man1/rvi.1.gz

Target path is vim.1.gz

/usr/man/man1/vi.1.gz

Target path is vim.1.gz

/usr/adm/sm.bin/wrapper

Target path is /usr/local/majordomo/wrapper

---

## 5.3 Check Name file-all-17

**Description**

Filenames consist of characters from a invalid range, and contain strange strings

**Consequences**

Although an unusual filename does not constitute a security problem in itself, it does increase the possibility of being mislead as to the contents of a directory. For example, it is possible that a directory with a name such as ".. " (note the space) could to be created in an uploadable ftp area and used to store illegal files, (such as illegitimate copies of software).

**Remedy**

Check all occurrences of strange file names and unless they have to be set to those values change them. Files can be removed using the “**rm**” command or moved with the “**mv**” command. Backslashes or Control-V can be used to escape unprintable characters, and wildcards may be used for characters that cannot be input using the keyboard.

**Vulnerability Detail**

**Files Affected**

/home/users/admin/Network Trash Folder

/usr/bin/[

/usr/man/man1/..1.gz

/usr/sausalito/codb/objects/0/CLASS=System

/usr/sausalito/codb/objects/0/CLASS=Network

/usr/sausalito/codb/objects/0/CLASS=User

/usr/sausalito/codb/objects/0/CLASS=Workgroup

/usr/sausalito/codb/objects/0/CLASS=Package

/usr/sausalito/codb/objects/0/CLASS=SWUpdateServer

/usr/sausalito/codb/objects/0/CLASS=ActiveMonitor

---

## Risk Level

## Medium

---

## 5.4 Check Name file-all-09

### Description

Files have “world” write permissions

### Consequences

Most files on the system should be controlled in such a way that only a specific group(s) of users can make changes to the file. There are exceptions, but these should be taken care of using the baseline facility.

### Remedy

If a file does not need to be world writable, it should be changed. Use the chmod o-w <filename> command to do so. The files that specifically should not be world writable are listed below.

**Vulnerability Detail**

**Files Affected**

/var/tmp
/var/lib/mysql/mysql.sock
/home/tmp
/usr/sausalito/cced.socket
/dev/ptmx

---

## 5.5 Check Name file-all-14

**Description**

Files are group writeable and can be (potentially) modified by group members.

**Consequences**

If files are group writeable there is a greater potential for corruption than if only the file owner has write permission. Often, files are made group writeable so that several people can work on the same project. However, some files, such as .cshrc and .profile, should never be group writeable.

**Remedy**

Ensure that only those files that need to be written to by members of a group have group write permissions. Also, check that all the users within the group need to be able to write to the object. You can use the command chmod g-w filename to remove write permissions from the file. The list of files, symbolic links, and directories below should have group write permission removed.

**Vulnerability Detail**

**Files Affected**

| | |
|---|---|
| /var/tmp | /var/lock/subsys: directory |
| /var/tmp: sticky directory | /var/run/utmp |
| /var/lib/mysql/mysql.sock | /var/run/utmp: data |
| /var/lib/mysql/mysql.sock: socket | /var/catman |
| /var/lib/mysql/10.0.0.19.pid | var/catman: directory |
| /var/lib/mysql/10.0.0.19.pid: ASCII text | /var/catman/X11R6 |
| /var/log/wtmp | /var/catman/X11R6: directory |
| /var/log/wtmp: data | /var/catman/X11R6/cat1 |
| /var/log/wtmp.1 | /var/catman/X11R6/cat1: directory |
| /var/log/wtmp.1: data | /var/catman/X11R6/cat2 |
| /var/lock | /var/catman/X11R6/cat2: directory |
| /var/lock: directory | /var/catman/X11R6/cat3 |
| /var/lock/subsys | /var/catman/X11R6/cat3: directory |
| /var/catman/X11R6/cat4 | /home/mgmt/db/mgmt/performance_fs_usage.frm |
| /var/catman/X11R6/cat4: directory | /home/mgmt/db/mgmt/performance_fs_usage.frm: data |

| | |
|---|---|
| /var/catman/X11R6/cat5 | /home/mgmt/db/mgmt/performance_fs_usage.MYI |
| /var/catman/X11R6/cat5: directory | /home/mgmt/db/mgmt/performance_fs_usage.MYI: data |
| /var/catman/X11R6/cat6 | /home/mgmt/db/mgmt/performance_fs_usage.MYD |
| /var/catman/X11R6/cat6: directory | /home/mgmt/db/mgmt_mysql.pid: ASCII text |
| | /home/mgmt/db/mgmt/inventory_os.MYD: empty |
| /var/catman/X11R6/cat7 | /home/mgmt/db/mgmt/inventory_cpu.frm |
| /var/catman/X11R6/cat7: directory | /home/mgmt/db/mgmt/inventory_cpu.frm: data |
| /var/catman/X11R6/cat8 | /home/mgmt/db/mgmt/inventory_cpu.MYI |
| /var/catman/X11R6/cat8: directory | /home/mgmt/db/mgmt/inventory_cpu.MYI: data |
| /var/catman/X11R6/cat9 | /home/mgmt/db/mgmt/inventory_cpu.MYD |
| /var/catman/X11R6/cat9: directory | /home/mgmt/db/mgmt/inventory_cpu.MYD: empty |
| /var/catman/X11R6/catn | /home/mgmt/db/mgmt/inventory_memory.frm |
| /var/catman/X11R6/catn: directory | /home/mgmt/db/mgmt/inventory_memory.frm: data |
| /var/catman/cat1 | /home/mgmt/db/mgmt/inventory_memory.MYI |
| /var/catman/cat1: directory | /home/mgmt/db/mgmt/inventory_memory.MYI: data |
| /var/catman/cat2 | /home/mgmt/db/mgmt/inventory_memory.MYD |
| /var/catman/cat2: directory | /home/mgmt/db/mgmt/inventory_memory.MYD: empty |
| /var/catman/cat3 | /home/mgmt/db/mgmt/inventory_nic.frm |
| /var/catman/cat3: directory | /home/mgmt/db/mgmt/inventory_nic.frm: data |
| /var/catman/cat4 | /home/mgmt/db/mgmt/inventory_nic.MYI |
| /var/catman/cat4: directory | /home/mgmt/db/mgmt/inventory_nic.MYI: data |
| /var/catman/cat5 | /home/mgmt/db/mgmt/inventory_nic.MYD |
| /var/catman/cat5: directory | /home/mgmt/db/mgmt/inventory_nic.MYD: empty |
| /var/catman/cat6 | /home/mgmt/db/mgmt/inventory_fs.frm |
| /var/catman/cat6: directory | /home/mgmt/db/mgmt/inventory_fs.frm: data |
| /var/catman/cat7 | /home/mgmt/db/mgmt/inventory_fs.MYI |
| /var/catman/cat7: directory | /home/mgmt/db/mgmt/inventory_fs.MYI: data |
| /var/catman/cat8 | /home/mgmt/db/mgmt/inventory_fs.MYD |
| /var/catman/cat8: directory | /home/mgmt/db/mgmt/inventory_fs.MYD: empty |
| /var/catman/cat9 | /home/mgmt/db/mgmt/performance_uptime.frm |
| /var/catman/cat9: directory | /home/mgmt/db/mgmt/performance_uptime.frm: data |
| /var/catman/cat3: directory | /home/mgmt/db/mgmt/performance_uptime.MYI |
| /var/catman/cat4 | /home/mgmt/db/mgmt/performance_uptime.MYI: data |
| /var/catman/cat4: directory | /home/mgmt/db/mgmt/performance_uptime.M |

| | |
|---|---|
| | YD |
| /var/catman/cat5 | /home/mgmt/db/mgmt/performance_uptime.MYD: empty |
| /var/catman/cat5: directory | /home/redhat/SOURCES/gnupg-1.0.4.tar.gz |
| /var/catman/cat6 | /home/redhat/SOURCES/gnupg-1.0.4.tar.gz: gzip compressed data, deflated, last modified: Tue Oct 17 09:40:57 2000, max compression, os: Unix |
| /var/catman/cat6: directory | /home/redhat/SPECS/openssh.spec |
| /var/catman/cat7 | /home/redhat/SPECS/openssh.spec: English text |
| /var/catman/cat7: directory | /home/redhat/SPECS/gnupg.spec |
| /var/catman/cat8 | /home/redhat/SPECS/gnupg.spec: English text |
| /var/catman/cat8: directory | /tmp |
| /var/catman/cat9 | /tmp: sticky directory |
| /var/catman/cat9: directory | /etc/rc.d/init.d/admserv |
| /var/catman/catn | /etc/rc.d/init.d/admserv: Bourne shell script text |
| /var/catman/catn: directory | /etc/rc.d/init.d/atalk |
| /var/catman/local | /etc/rc.d/init.d/atalk: Bourne shell script text |
| /var/catman/local: directory | /etc/rc.d/init.d/httpd |
| /var/catman/local/cat1 | /etc/rc.d/init.d/httpd: Bourne shell script text |
| /var/catman/local/cat1: directory | /etc/rc.d/init.d/named |
| /var/catman/local/cat2 | /etc/rc.d/init.d/named: Bourne shell script text |
| /var/catman/local/cat2: directory | /etc/rc.d/init.d/nfsfs |
| /var/catman/local/cat3 | /etc/rc.d/init.d/nfsfs: Bourne shell script text |
| /var/catman/local/cat3: directory | /etc/rc.d/init.d/postgresql |
| /var/catman/local/cat4 | /etc/rc.d/init.d/postgresql: Bourne-Again shell script text |
| /var/catman/local/cat4: directory | /etc/rc.d/init.d/quota |
| /var/catman/local/cat5 | /etc/rc.d/init.d/quota: Bourne shell script text |
| /var/catman/local/cat5: directory | /etc/rc.d/init.d/sendmail |
| /var/catman/local/cat6 | /etc/rc.d/init.d/sendmail: Bourne shell script text |
| /var/catman/local/cat6: directory | /etc/rc.d/init.d/smb |
| /var/catman/local/cat7 | /etc/rc.d/init.d/smb: Bourne shell script text |
| /var/catman/local/cat7: directory | /etc/rc.d/init.d/snmpd |
| /var/catman/local/cat8 | /etc/rc.d/init.d/snmpd: Bourne-Again shell script text |
| /var/catman/local/cat8: directory | /etc/admserv/certs/key |
| /var/catman/local/cat9 | /etc/admserv/certs/key: ASCII text |
| /var/catman/local/cat9: directory | /etc/admserv/certs/request |
| /var/catman/local/catn | /etc/admserv/certs/request: ASCII text |
| /var/catman/local/catn: directory | /etc/admserv/certs/certificate |
| /home/tmp | /etc/admserv/certs/certificate: ASCII text |
| /home/tmp: sticky directory | /etc/httpd/ssl/key |
| /home/mgmt/db/mgmt/mgmt_build.frm | /etc/httpd/ssl/key: ASCII text |
| /home/mgmt/db/mgmt/mgmt_build.frm: data | /etc/httpd/ssl/request |
| /home/mgmt/db/mgmt/mgmt_build.MYI | /etc/httpd/ssl/request: ASCII text |
| /home/mgmt/db/mgmt/mgmt_build.MYI: | /etc/httpd/ssl/certificate |

| | |
|---|---|
| data | |
| /home/mgmt/db/mgmt/mgmt_build.MYD | /etc/httpd/ssl/certificate: ASCII text |
| /home/mgmt/db/mgmt/mgmt_build.MYD: ASCII text (with escape sequences) | /mnt/cdrom |
| /home/mgmt/db/mgmt/mgmt_appliance.frm | /mnt/cdrom: directory |
| /home/mgmt/db/mgmt/mgmt_appliance.frm: data | /mnt/floppy |
| /home/mgmt/db/mgmt/mgmt_appliance.MYI | /mnt/floppy: directory |
| /home/mgmt/db/mgmt/mgmt_appliance.MYI: data | /usr/include/python1.5 |
| /home/mgmt/db/mgmt/mgmt_appliance.MYD | /usr/include/python1.5: directory |
| /home/mgmt/db/mgmt/mgmt_appliance.MYD: empty | /usr/lib/python1.5 |
| /home/mgmt/db/mgmt/mgmt_mapp.frm | /usr/lib/python1.5: directory |
| /home/mgmt/db/mgmt/mgmt_mapp.frm: data | /usr/lib/python1.5/lib-stdwin |
| /home/mgmt/db/mgmt/mgmt_mapp.MYI | /usr/lib/python1.5/lib-stdwin: directory |
| /home/mgmt/db/mgmt/mgmt_mapp.MYI: data | /usr/lib/python1.5/test |
| /home/mgmt/db/mgmt/mgmt_mapp.MYD | /usr/lib/python1.5/test: directory |
| /home/mgmt/db/mgmt/mgmt_mapp.MYD: data | /usr/lib/python1.5/test/output |
| /home/mgmt/db/mgmt/mgmt_mapp_client_rpm.frm | /usr/lib/python1.5/test/output: directory |
| /home/mgmt/db/mgmt/mgmt_mapp_client_rpm.frm: data | /usr/lib/python1.5/plat-linux-i386 |
| /home/mgmt/db/mgmt/mgmt_mapp_client_rpm.MYI | /usr/lib/python1.5/plat-linux-i386: directory |
| /home/mgmt/db/mgmt/mgmt_mapp_client_rpm.MYI: data | /usr/lib/python1.5/config |
| /home/mgmt/db/mgmt/mgmt_mapp_client_rpm.MYD | /usr/lib/python1.5/config: directory |
| /home/mgmt/db/mgmt/mgmt_mapp_client_rpm.MYD: data | /usr/lib/authenticate |
| /home/mgmt/db/mgmt/mgmt_mapp_server_rpm.frm | /usr/lib/authenticate: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped |
| /home/mgmt/db/mgmt/mgmt_mapp_server_rpm.frm: data | /usr/sausalito/cced.socket |
| /home/mgmt/db/mgmt/mgmt_mapp_server_rpm.MYI | /usr/sausalito/cced.socket: socket |
| /home/mgmt/db/mgmt/mgmt_mapp_server_rpm.MYI: data | /dev/null |
| /home/mgmt/db/mgmt/mgmt_mapp_server_rpm.MYD | /dev/null: character special (1/3) |
| /home/mgmt/db/mgmt/mgmt_mapp_server_rpm.MYD: ASCII text | /dev/atibm |
| /home/mgmt/db/mgmt/mgmt_installed_rpm.frm | /dev/atibm: character special (10/3) |

| | |
|---|---|
| /home/mgmt/db/mgmt/mgmt_installed_rpm.frm: data | /dev/aztcd |
| /home/mgmt/db/mgmt/mgmt_installed_rpm.MYI | /dev/aztcd: block special (29/0) |
| /home/mgmt/db/mgmt/mgmt_installed_rpm.MYI: data | /dev/bpcd |
| /home/mgmt/db/mgmt/mgmt_installed_rpm.MYD | /dev/bpcd: block special (41/0) |
| /home/mgmt/db/mgmt/mgmt_installed_rpm.MYD: empty | /dev/cdu31a |
| /home/mgmt/db/mgmt/mgmt_view.frm | /dev/cdu31a: block special (15/0) |
| /home/mgmt/db/mgmt/mgmt_view.frm: data | /dev/cm206cd |
| /home/mgmt/db/mgmt/mgmt_view.MYI | /dev/cm206cd: block special (32/0) |
| /home/mgmt/db/mgmt/mgmt_view.MYI: data | /dev/cui0 |
| /home/mgmt/db/mgmt/mgmt_view.MYD | /dev/cui0: character special (44/0) |
| /home/mgmt/db/mgmt/mgmt_view.MYD: empty | /dev/cui1 |
| /home/mgmt/db/mgmt/mgmt_view_to_appliance.frm | /dev/cui1: character special (44/1) |
| /home/mgmt/db/mgmt/mgmt_view_to_appliance.frm: data | /dev/cui10 |
| /home/mgmt/db/mgmt/mgmt_view_to_appliance.MYI | /dev/cui10: character special (44/10) |
| /home/mgmt/db/mgmt/mgmt_view_to_appliance.MYI: data | /dev/cui11 |
| /home/mgmt/db/mgmt/mgmt_view_to_appliance.MYD | /dev/cui11: character special (44/11) |
| /home/mgmt/db/mgmt/mgmt_view_to_appliance.MYD: empty | /dev/cui12 |
| /home/mgmt/db/mgmt/mgmt_appliance_status.frm | /dev/cui12: character special (44/12) |
| /home/mgmt/db/mgmt/mgmt_appliance_status.frm: data | /dev/cui13 |
| /home/mgmt/db/mgmt/mgmt_appliance_status.MYI | /dev/cui13: character special (44/13) |
| /home/mgmt/db/mgmt/mgmt_appliance_status.MYI: data | /dev/cui14 |
| /home/mgmt/db/mgmt/mgmt_appliance_status.MYD | /dev/cui14: character special (44/14) |
| /home/mgmt/db/mgmt/mgmt_appliance_status.MYD: data | /dev/cui15 |
| /home/mgmt/db/mgmt/mgmt_config.frm | /dev/cui15: character special (44/15) |
| /home/mgmt/db/mgmt/mgmt_config.frm: data | /dev/cui16 |
| /home/mgmt/db/mgmt/mgmt_config.MYI | /dev/cui16: character special (44/16) |
| /home/mgmt/db/mgmt/mgmt_config.MYI: data | /dev/cui17 |
| /home/mgmt/db/mgmt/mgmt_config.MYD | /dev/cui17: character special (44/17) |
| /home/mgmt/db/mgmt/mgmt_config.MYD: ASCII text | /dev/cui18 |
| /home/mgmt/db/mgmt/mgmt_task.frm | /dev/cui18: character special (44/18) |

| | |
|---|---|
| /home/mgmt/db/mgmt/mgmt_task.frm: data | /dev/cui19 |
| /home/mgmt/db/mgmt/mgmt_task.MYI | /dev/cui19: character special (44/19) |
| /home/mgmt/db/mgmt/mgmt_task.MYI: data | /dev/cui2 |
| /home/mgmt/db/mgmt/mgmt_task.MYD | /dev/cui2: character special (44/2) |
| /home/mgmt/db/mgmt/mgmt_task.MYD: data | /dev/cui20 |
| /home/mgmt/db/mgmt/mgmt_event.frm | /dev/cui20: character special (44/20) |
| /home/mgmt/db/mgmt/mgmt_event.frm: data | /dev/cui21 |
| /home/mgmt/db/mgmt/mgmt_event.MYI | /dev/cui21: character special (44/21) |
| /home/mgmt/db/mgmt/mgmt_event.MYI: data | /dev/cui22 |
| /home/mgmt/db/mgmt/mgmt_event.MYD | /dev/cui22: character special (44/22) |
| /home/mgmt/db/mgmt/mgmt_event.MYD: data | /dev/cui23 |
| /home/mgmt/db/mgmt/mgmt_ignore_appliance.frm | /dev/cui23: character special (44/23) |
| /home/mgmt/db/mgmt/mgmt_ignore_appliance.frm: data | /dev/cui24 |
| /home/mgmt/db/mgmt/mgmt_ignore_appliance.MYI | /dev/cui24: character special (44/24) |
| /home/mgmt/db/mgmt/mgmt_ignore_appliance.MYI: data | /dev/cui25 |
| /home/mgmt/db/mgmt/mgmt_ignore_appliance.MYD | /dev/cui25: character special (44/25) |
| /home/mgmt/db/mgmt/mgmt_ignore_appliance.MYD: empty | /dev/cui26 |
| /home/mgmt/db/mgmt/health_service.frm | /dev/cui26: character special (44/26) |
| /home/mgmt/db/mgmt/health_service.frm: data | /dev/cui27 |
| /home/mgmt/db/mgmt/health_service.MYI | /dev/cui27: character special (44/27) |
| /home/mgmt/db/mgmt/health_service.MYI: data | /dev/cui28 |
| /home/mgmt/db/mgmt/health_service.MYD | /dev/cui28: character special (44/28) |
| /home/mgmt/db/mgmt/health_service.MYD: ASCII text | /dev/cui29 |
| /home/mgmt/db/mgmt/health_state.frm | /dev/cui29: character special (44/29) |
| /home/mgmt/db/mgmt/health_state.frm: data | /dev/cui3 |
| /home/mgmt/db/mgmt/health_state.MYI | /dev/cui3: character special (44/3) |
| /home/mgmt/db/mgmt/health_state.MYI: data | /dev/cui30 |
| /home/mgmt/db/mgmt/health_state.MYD | /dev/cui30: character special (44/30) |
| /home/mgmt/db/mgmt/health_state.MYD: empty | /dev/cui31 |
| /home/mgmt/db/mgmt/swmgmt_pkgs.frm | /dev/cui31: character special (44/31) |
| /home/mgmt/db/mgmt/swmgmt_pkgs.frm: data | /dev/cui32 |
| /home/mgmt/db/mgmt/swmgmt_pkgs.MYI | /dev/cui32: character special (44/32) |

| | |
|---|---|
| /home/mgmt/db/mgmt/swmgmt_pkgs.MYI: data | |
| /home/mgmt/db/mgmt/swmgmt_pkgs.MYD | |
| /home/mgmt/db/mgmt/swmgmt_pkgs.MYD: empty | |
| /home/mgmt/db/mgmt/swmgmt_installedsw.frm | |
| /home/mgmt/db/mgmt/swmgmt_installedsw.frm: data | |
| /home/mgmt/db/mgmt/swmgmt_installedsw.MYI | |
| /home/mgmt/db/mgmt/swmgmt_installedsw.MYI: data | |
| /home/mgmt/db/mgmt/swmgmt_installedsw.MYD | |
| /home/mgmt/db/mgmt/swmgmt_installedsw.MYD: empty | |
| /home/mgmt/db/mgmt/swmgmt_servers.frm | |
| /home/mgmt/db/mgmt/swmgmt_servers.frm: data | |
| /home/mgmt/db/mgmt/swmgmt_servers.MYI | |
| /home/mgmt/db/mgmt/swmgmt_servers.MYI: data | |
| /home/mgmt/db/mgmt/swmgmt_servers.MYD | |
| /home/mgmt/db/mgmt/swmgmt_servers.MYD: empty | |
| /home/mgmt/db/mgmt/swmgmt_config.frm | |
| /home/mgmt/db/mgmt/swmgmt_config.frm: data | |
| /home/mgmt/db/mgmt/swmgmt_config.MYI | |
| /home/mgmt/db/mgmt/swmgmt_config.MYI: data | |
| /home/mgmt/db/mgmt/swmgmt_config.MYD | |
| /home/mgmt/db/mgmt/swmgmt_config.MYD: data | |
| /home/mgmt/db/mgmt/inventory_os.frm | |
| /home/mgmt/db/mgmt/inventory_os.frm: data | |
| /home/mgmt/db/mgmt/inventory_os.MYI | |
| /home/mgmt/db/mgmt/inventory_os.MYI: data | |
| /home/mgmt/db/mgmt/inventory_os.MYD | |

## 5.6 Check Name file-all-16

**Description**

Files within directories have an owner different from the owner of the directory.

**Consequences**

If a file has an owner that is different from the owner of the directory in which it exists, it may be that it has been placed there inadvertently by another user, (such as root), allowing the directory owner to remove it when perhaps they should not.

**Remedy**

Check the reason for the file having a different owner since there are examples where such practice is unavoidable and intentional, such as /tmp. However, in general, it is best to try to ensure that the files within a directory are owned by the user. In the case of a file within a user's home directory area, perhaps modify the permissions to stop them from removing files owned by root, if possible. Changes in file ownership can be performed using the chown command.

**Vulnerability Detail**

**Files Impacted**

| | | | |
|---|---|---|---|
| /home/spool/mail/admin | | | |
| Directory | root | mail | rwxrwxr-x |
| /home/log/httpd/adm_ssl_mutex.635 | | | |
| Directory | root | root | rwxr-xr-x |
| /home/log/httpd/adm_ssl_scache.pag | | | |
| Directory | root | root | rwxr-xr-x |
| /home/log/httpd/adm_ssl_scache.dir | | | |
| Directory | root | root | rwxr-xr-x |
| /home/groups/home/web/splashDefaultWeb.jpg | | | |
| Directory | admin | home | rwxrwsr-x |
| /tmp/sess_4b2e695f31f7556f667e55847f634802 | | | |
| Directory | root | root | rwxrwxrwx |

---

## 5.7 Check Name file-sgid-binary

**Description**

Binary files have the setgid bit set

**Consequences**

SGID executables change the group ID of their process to match executable's group, and execute with the access permissions of the group that owns the script. If an attacker is able to modify a SGID program, or is able to change some other program executed by it, then the attacker can execute arbitrary code on the system with access permissions of the program itself. This is particularly dangerous if the owning group is root.

**Remedy**

Many common system executables are SGID root and are not security risks on the basis of being SGID alone. However, such programs are often found to have bugs that allow them to be exploited to gain root access.

Ensure that the file permissions, user and groups are set to allow the correct level of access to certain objects for a specified set of users. The chmod command can be used to establish the appropriate level of access or set or unset the setgid bit.

A user on the system should not, in general, need to be in possession of an SGID binary. Such an executable found in a user`s home directory should be considered suspect.

**Vulnerability Details**
**Files Impacted**

```
/usr/bin/wall

  /usr/bin/wall: setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/man

  /usr/bin/man: setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/slocate

  /usr/bin/slocate: setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/write

  /usr/bin/write: setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/mutt_dotlock

  /usr/bin/mutt_dotlock: setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/lockfile

  /usr/bin/lockfile: setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/procmail

  /usr/bin/procmail: setuid setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/lib/emacs/20.5/i386-redhat-linux-gnu/movemail
```

```
  /usr/lib/emacs/20.5/i386-redhat-linux-gnu/movemail: setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped
```

---

## 5.8 Check Name file-sgid-script

### Description

Script files have the setgid bit set

### Consequences

A file with a setgid bit set executes with the permissions of the owning group. If an attacker or user is able to modify a SGID script, or is able to change some other script or program that the script executes, then the attacker can execute arbitrary code on the system with access permissions of the program itself. This is particularly dangerous if the owning group is root.

### Remedy

Closely examine a script that is set to run SGID with a text viewer to verify that is is not doing anything questionable (such as making a copy of /bin/sh). Ensure that the file permissions, user and groups are set to allow the correct level of access to certain objects for a specified set of users. The chmod command can be used to establish the appropriate level of access or set or unset the setgid bit.

### Vulnerability Details
### Files Impacted

```
/home/groups/home

  /home/groups/home: setgid directory

/home/groups/home/web

  /home/groups/home/web: setgid directory

/home/groups/restore

  /home/groups/restore: setgid directory

/home/groups/restore/web

  /home/groups/restore/web: setgid directory

/home/users/admin

  /home/users/admin: setgid directory

/home/users/admin/Network Trash Folder

  /home/users/admin/Network Trash Folder: setgid directory

/usr/doc/python-docs-1.5.2/Doc

  /usr/doc/python-docs-1.5.2/Doc: setgid directory
```

/usr/doc/python-docs-1.5.2/Doc/icons

/usr/doc/python-docs-1.5.2/Doc/icons: setgid directory

/usr/doc/python-docs-1.5.2/Doc/ref

/usr/doc/python-docs-1.5.2/Doc/ref: setgid directory

---

## 5.9 Check Name file-suid-binary

**Description**

Binary files have the setuid bit set

**Consequences**

SUID executables change the user ID of their process to match the executable's owner, and execute with the access permissions of the user that owns the script. If an attacker is able to modify a SUID program, or is able to change some other program executed by it, then the attacker can execute arbitrary code on the system with access permissions of the program itself. This is particularly dangerous if the owning user is root.

**Remedy**

Many common system executables (such as sendmail, rlogin, rsh) are SUID root and are not security risks on the basis of being SUID alone. However, such programs are often found to have bugs that allow them to be exploited to gain root access. Consult a security mailing list or FTP archive site for your operating system for information on SUID binaries. Apply any appropriate patches or mode changes prescribed for vulnerable programs on your system.

Ensure that the file permissions, user and groups are set to allow the correct level of access to certain objects for a specified set of users. The chmod command can be used to establish the appropriate level of access or set or unset the setuid bit.

A user on the system should not, in general, need to be in possession of an SUID binary. Such an executable found in a user`s home directory should be considered suspect.

**Vulnerability Details**
**Files Impacted**

/bin/mount

/bin/mount: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/bin/umount

/bin/umount: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/bin/ping

```
  /bin/ping: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/bin/su

  /bin/su: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/sbin/pwdb_chkpwd

  /sbin/pwdb_chkpwd: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped

/sbin/unix_chkpwd

  /sbin/unix_chkpwd: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped

/usr/bin/chage

  /usr/bin/chage: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/gpasswd

  /usr/bin/gpasswd: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/passwd

  /usr/bin/passwd: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/rcp

  /usr/bin/rcp: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/rlogin

  /usr/bin/rlogin: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/rsh

  /usr/bin/rsh: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/chfn

  /usr/bin/chfn: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/newgrp

  /usr/bin/newgrp: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/crontab

  /usr/bin/crontab: setuid ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped
```

```
/usr/bin/procmail

  /usr/bin/procmail: setuid setgid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/bin/at

  /usr/bin/at: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/lib/authenticate

  /usr/lib/authenticate: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped

/usr/sbin/cmos

  /usr/sbin/cmos: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped

/usr/sbin/traceroute

  /usr/sbin/traceroute: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/sbin/fpexec

  /usr/sbin/fpexec: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped

/usr/sbin/suexec

  /usr/sbin/suexec: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/sbin/sendmail

  /usr/sbin/sendmail: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), stripped

/usr/libexec/pt_chown

  /usr/libexec/pt_chown: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped

/usr/sausalito/bin/ccewrap

  /usr/sausalito/bin/ccewrap: setuid ELF 32-
bit LSB executable, Intel 80386, version 1, dynamically linked (uses shared libs), not stripped
```

During the course of this phase of the Big Daddy Assessment, it was discovered that the database application MySQL was being used to house the information generated from our management console. Given the history of security issues of other well known database applications, it is the intent of the Columbus Security Engineering VA Team to conduct additional research into the MySQL database application as it relates to known security vulnerabilities. The results of this additional research will be presented under separate cover.

Distribution: Stephen Harpster
Larry Coryell
CSE Managers

Charles Smith
Project Manager
Tel: 614 273 3255
Email: charles.smith@sun.com