Project Name: Vulnerability Assessment Big Daddy

Application Based Information Security Vulnerability Assessment of the Big Daddy Appliance

Prepared By Charles Smith 31 January 2002

Document Review

Name	Role	Review Date
Charles Smith	Project Manager	01/31/02
Shaun White	Manager (Security)	02/01/02
Larry Coryell	Project Manager Big Daddy	

References: See References

Distribution: See Distribution

Sun Microsystems, Inc

Cobalt Server Appliance Business Unit

1160 Dublin Road

Columbus, OH 43215

1 Modification Log

Author	Version	Date	Comment
Charles Smith	1.0	01/31/02	Release

Table of Contents

2 Purpose

To provide management part III of the three-part Big Daddy vulnerability assessment (VA) project, an application based VA assessment, conducted by the Vulnerability Assessment Team, Columbus Security Engineering Group.

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

The assessment criteria used to compile this baseline was derived from the identification of known application level threats and an analysis of the impact of the identified threats against the Big Daddy appliance 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 application 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 or deny use of the system by way of successful denial of service attacks. Medium risk vulnerabilities provide access to sensitive network data that may lead to the exploration of higher risk vulnerabilities. Low risk vulnerabilities provide access to sensitive, yet non-lethal, network 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.

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

Risk Level	Description
MEDIUM	5.1 - EXPOSURE OF INFORMATION BY INCREMENTING OR DECREMENTING A PARAMETER'S VALUE

5 Appendix B – Full Discussion of Issues

Risk Level
Medium

5.1 EXPOSURE OF INFORMATION (BY INCREMENTING/DECREMENTING A PARAMETER'S VALUE

Description

If the attacker probes the application by forging a request that contains a parameter value that has been incremented or decremented from its original value, the application may enter an undefined state that makes it vulnerable to attack. The attacker can gain useful information from the application's response to this request that may be exploited to locate application weaknesses.

Consequences

By incrementing/decrementing a parameter's value, an attacker can gain useful information about the behavior of the application, or even gain data that was supposed to be confidential.

Remedy

Check that all parameter values are in their expected range. When a value is out of range, issue an error message or use default values.

Links Affected:

Original Link:
http://test1.va.org/base/appmgr/groups.php?action=add&gotSelect=1&name=workgroup&description=workgroup

Mutated Link:
http://test1.va.org/base/appmgr/groups.php?action=add&description=workgroup&gotSelect=2&name=workgroup

Original Link:
http://test1.va.org/base/appmgr/groups.php?action=addform&modify=1&id=1&name=workgroup&num=&description=workgroup

Mutated Link:
http://test1.va.org/base/appmgr/groups.php?action=addform&description=workgroup&id=1&modify=2&name=workgroup&num=

Original Link:
http://test1.va.org/base/appmgr/groups.php?action=list&id=1&name=workgroup

Mutated Link:
http://test1.va.org/base/appmgr/groups.php?action=list&id=2&name=workgroup

Original Link:
http://test1.va.org/base/mgmt-swmgmt/settings.php?action=addform&modify=1&id=1

Mutated Link:
http://test1.va.org/base/mgmt-swmgmt/settings.php?action=addform&id=1&modify=2

Original Link:
http://test1.va.org/base/mgmt-health/viewalarms.php?group=1&name=workgroup

Mutated Link:
http://test1.va.org/base/mgmt-health/viewalarms.php?group=2&name=workgroup

Original Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=3&name=Appliance+Inventory

Mutated Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=4&name=Appliance+Inventory

Original Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=1&name=Health+Monitoring

Mutated Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=2&name=Health+Monitoring

Original Link:
http://test1.va.org/base/network/routes.php?ADD=1

Mutated Link:
http://test1.va.org/base/network/routes.php?ADD=2

Original Link:
http://test1.va.org/base/appmgr/groups.php?action=add&gotSelect=1&name=workgroup&description=workgroup

Mutated Link:
http://test1.va.org/base/appmgr/groups.php?action=add&description=workgroup&gotSelect=0&name=workgroup

Original Link:
http://test1.va.org/base/appmgr/groups.php?action=addform&modify=1&id=1&name=workgroup&num=&description=workgroup

Mutated Link:
http://test1.va.org/base/appmgr/groups.php?action=addform&description=workgroup&id=1&modify=0&name=workgroup&num=

Original Link:
http://test1.va.org/base/appmgr/groups.php?action=addform&modify=1&id=1&name=workgroup&num=&description=workgroup

Mutated Link:
http://test1.va.org/base/appmgr/groups.php?action=addform&description=workgroup&id=0&modify=1&name=workgroup&num=

Original Link:
http://test1.va.org/base/appmgr/groups.php?action=list&id=1&name=workgroup

Mutated Link:
http://test1.va.org/base/appmgr/groups.php?action=list&id=0&name=workgroup

Original Link:
http://test1.va.org/base/mgmt-swmgmt/settings.php?action=addform&id=1&modify=1

Mutated Link:
http://test1.va.org/base/mgmt-swmgmt/settings.php?action=addform&id=1&modify=0

Original Link:
http://test1.va.org/base/mgmt-swmgmt/settings.php?action=addform&modify=1&id=1

Mutated Link:
http://test1.va.org/base/mgmt-swmgmt/settings.php?action=addform&modify=1&id=0

Original Link:
http://test1.va.org/base/mgmt-health/viewalarms.php?group=1&name=workgroup

Mutated Link:
http://test1.va.org/base/mgmt-health/viewalarms.php?group=0&name=workgroup

Original Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=3&name=Appliance+Inventory

Mutated Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=2&name=Appliance+Inventory

Original Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=1&name=Health+Monitoring

Mutated Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=0&name=Health+Monitoring

Original Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=2&name=Software+Management

Mutated Link:
http://test1.va.org/base/mgmtapp/installedAppliances.php?id=1&name=Software+Management

Original Link:
http://test1.va.org/base/network/routes.php?ADD=1

Mutated Link:
http://test1.va.org/base/network/routes.php?ADD=0

Distribution: Stephen Harpster
Larry Coryell
CSE Managers

Charles Smith

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