SECURITY ASSESSMENT: Bomgar Appliances

Bomgar

Bomgar Appliance Penetration Test

March 2013

Table of Contents

Introduction

During the period between November 2012 and March 2013, Symantec Consulting Services partnered with Bomgar to assess the security architecture and implementation of the Bomgar appliances. During the engagement, Symantec performed a Product Penetration Test to evaluate the application components and related environment against established security best practices.

A Product Penetration Test is designed to provide insight into methods of attack against a specific product or suite of applications and present a reasonable example of what an attacker might accomplish. The assessment concentrates on modeling specific attack scenarios, identifying vulnerabilities, and validating exploitation possibilities. The findings presented in this document are accurate as of the time of writing and are the opinion of Symantec; as both products and security technologies evolve, these statements may or may not be applicable to future releases and Symantec does not guarantee future accuracy of these statements.

Executive Summary

Symantec conducted the Product Penetration Test to evaluate the security architecture of the Bomgar appliance and supporting components in order to identify security vulnerabilities that might pose risk to Bomgar's customers. The purpose of this test was to ascertain the security posture of the targeted product from a hacker's or a malicious user's perspective and determine what, if any, resources could be compromised through attacks on confidentiality, integrity, or availability.

During the assessment, Symantec found the overall architecture of the Bomgar appliances to be designed and implemented with security best practices in mind. Although initial testing was performed on Bomgar B200, B300, and B400 appliances running version 12.3 software, the findings in this document should pertain to any Bomgar Box appliance running firmware version 3.3 and 3.4 with the latest maintenance releases as of April 2013 applied.

Bomgar Application Environment Overview

The Bomgar environment consists of the following key components:

- **Bomgar Appliance**: The Bomgar appliance is a dedicated hardware box that supports Bomgar's base server components and administrative interfaces and acts as a centralized routing interface for all communication between support agents and end users.

- **Bomgar Representative Console**: The Bomgar Representative Console is a multi-platform application used by support desk agents to remotely access customer workstations and perform chat, file transfer, and remote management operations.

- **Bomgar Customer Client**: The customer client is a cross-platform executable that is downloaded during initiation of a support session and enables the support representative to gain remote access to the customer's workstation. Upon termination of the session, the program automatically uninstalls or can remain on the user's

workstation to support long running issues.

The scope of the assessment included the following Bomgar components and client operating systems:

- Bomgar Software: 12.3 - /login
- Bomgar Firmware: 3.3 - /appliance
- Bomgar Firmware: 3.4 - /appliance
- Bomgar Jumpoints
- Bomgar Jumpoints/vPro
- Bomgar Rep Console – Windows, Mac, Linux, iPhone, iPad, Android Phone, Android Tablet
- Bomgar Smart Card Support
- Bomgar Rep Invite
- Bomgar Customer Client – Windows, Mac, Linux, Blackberry, Windows Mobile, iPhone, iPad, Android Phone and Android Tablet
- Bomgar Jump Clients
- Bomgar Passive Jump Clients
- Bomgar Button
- Bomgar Connection Agent
- Bomgar Integration Client

Bomgar Security Architecture

During the assessment, Symantec reviewed the various Bomgar components and their interactions and how the complete solution worked to defend against attackers.

1. Bomgar Hardware

The tenants of security are the result of a secure foundation at the hardware layer.

The Bomgar appliances are shipped as self contained, hardened servers that utilize a minimal base firmware to help customers install the Bomgar solution. The servers have been hardened from both a software and physical level. The only access allowed to the device is through a private link local IP address preconfigured on the network interface adapters on the server. All USB ports are disabled through the BIOS and cannot be used for keyboards or mounting USB drives. The first step for installing the Bomgar solution is to update the base firmware to the latest version. Once this is in place an SSL certificate can either be imported or a certificate signing request can be generated through the firmware UI. With the base firmware updated, the latest Bomgar application can be downloaded and installed onto the appliance.

Symantec conducted port scans of the Bomgar appliance and found that four network ports were enabled in the default configuration. A review of the ports enabled on the Bomgar appliance revealed that three of the ports were for connectivity to HTTP (TCP 80), HTTPS (TCP 443) and an alternative HTTPS port (TCP 8200). The fourth port was for a custom telnet interface and was only accessible through the preconfigured link-local IP address (RFC 3927). RFC 3927 prohibits the routing of link local IP addresses, which limits the accessibility of the telnet interface to the underlying

VLAN/network segment that the network interface is connected to.

The web management interfaces, '/login' and '/appliance', required the use of HTTPS to access the administrative settings. The HTTP interface on port 80 can only be used by end users and is in place for the public interface to provide a default landing URI. This interface can be configured to automatically redirect the user to the HTTPS (SSL) Port within the security settings of the application administrative interface, '/login'.

Bomgar supports deployment of the Bomgar appliance to an external public network, a DMZ or an internal network. There are tradeoffs from both a security perspective and a configuration complexity to each of these scenarios and the final choice will be typically be a function of a customer's security policy, existing infrastructure and the location of the customer's user base relative to firewalls. There is nothing in the default configuration of the Bomgar appliance that would preclude recommending deployment of the appliance on an external network, outside of the corporate firewall.

Administrators are able to apply network restrictions to both the appliance administrative interface, '/appliance', and to the application administrative interface, '/login', and Symantec would recommend that this process is completed as soon as the deployment methodology has been determined.

During testing, Symantec found that the limited exposure of network services and general configuration of the device, successfully prevented access to the network interfaces of other internal server components, thus limiting possible attack vectors.

2. Communications Encryption

The key to securing any solution is to ensure that all components can communicate in a secure manner with one another and with the outside world.

To meet this goal Bomgar utilizes SSL encryption for all communication between the Bomgar appliance, representative consoles and customer clients. While the appliance allows the use of a self-signed certificate, Symantec strongly recommends that Bomgar customers utilize a recognized certificate authority such as VeriSign (owned by Symantec) or Entrust to sign their certificates.

The architecture of the Bomgar solution relies on the Bomgar appliance acting as a centralized routing point for all communications between application components. All Bomgar sessions between representatives and remote customers, Bomgar Jump Clients and Bomgar Jumpoints occur through the server components running on the Bomgar appliance. Data transmitted during these sessions includes customer screen data, login credentials and commands from the representative that result in remote control of the customer's workstation.

The Bomgar appliance ships with SSL version 2 disabled and by default only allows SSL ciphers with a key size of 128 bits or greater. Customers are allowed to modify the SSL configuration on the appliance through the administrative interface. The SSLv2 protocol contains design flaws and is generally considered insecure and should only be enabled if customers need to support legacy devices that do not support SSLv3 or TLS. All modern browsers, including those on mobile devices purchased in the last three years, support SSLv3 and TLSv1 and will not be adversely affected by the absence of SSLv2.

3. Authentication and Authorization

A well designed authentication and authorization mechanisms help to mitigate many key security risks.

The Bomgar application uses dedicated accounts for accessing server functionality and data. On startup the default administrator application password has to be changed. Customers have the ability to customize the password policy to ensure that is complies with their business security policy. The Bomgar application can be configured with a local user list or Bomgar users can also be authenticated via LDAP (to ActiveDirectory, Novell eDirectory or OpenLDAP), Kerberos or RADIUS. During the assessment, Symantec tested a variety of attack scenarios designed to circumvent the authentication mechanisms implemented in the Bomgar appliance. Symantec found that both the web-based and client-server interfaces to the Bomgar appliance back-end components required the user to successfully authenticate with a valid username and password. All attempts to bypass the authentication components were rejected by the application, thereby preventing unauthorized access to functionality and data on the server. The configured account lockout policy also worked as defined in the application security options.

Symantec also found that the Bomgar appliance supports a very granular level of user access controls. User privileges can be set through either a Bomgar group policy or on a per-user basis. When accounts are created, the administrator is presented with a list of privileges that can be selectively granted to the user, including the ability to view and/or control a customer's machine remotely or the ability to act as an administrator for the application. Customers should review the granularity of the controls offered and ensure that the range of group policies configured is commensurate with the scope and diversity of their supports teams and the activities they need to support. During the assessment, Symantec attempted to bypass access control functions and access functions and/or data that should have been restricted to more highly privileged users. These attempts were rejected by the access control mechanisms built into the solution.

The Bomgar appliance uses a separate administration account and interface to govern administration of the Bomgar server firmware. This provides additional segregation between user functions within the overall application environment.

4. Customer Client Security

In order to establish a Bomgar support session, the remote customer will download and run a small executable that will establish a connection back through the Bomgar appliance and link them with a support representative. The initial session provides a simple chat session that allows the support representative to securely communicate with the end users. If required, the support representative can request permission to see the end user's desktop through screen sharing, perform a file transfer, gain access to a command shell and view system information. By default each of these requested actions will prompt the end user whether they would like to allow or refuse the request. At any point the end user can click a large red X to stop any and all representative activity such as screen sharing. The customer is also given the option to terminate the support session completely and remove the client software.

Once a support session terminates, the client executable automatically terminates running processes related to the support session and uninstalls itself from the customer's workstation. Any subsequent support sessions will require the customer to rerun the installation process in order to deploy the customer client again on their workstation.

During the penetration test, Symantec noted that the access controls afforded to remote customers sufficiently restrict access to their workstation. Symantec was unable to obtain control over customer machines that were granted only viewing privileges and was not able to resume a support session once the session had been terminated and the client uninstalled.

5. Auditing and Logging

In a well designed system, logs are maintained in sufficient detail to permit reconstruction of system activity.

The Bomgar solution contains several logging functions. Configuration changes within the /appliance and /login web interfaces as well as representative console logins can be logged to a remote syslog when setup. By default all support sessions are logged locally on the appliance along with details of who the customer was and when events such as screen sharing occurred. This data along with the chat session can be viewed by all authorized users within the /login web interface. At the end of the support session the customer is allowed to view a copy of the chat transcript. Additionally session recording can be enabled for screen sharing, command shell access and presentations. The recordings can be played back or downloaded as Flash video files by authorized users.

Deployment Best Practices

Out of the box the Bomgar appliance represents a reasonable security profile that will resist most cyber attacks. Symantec recommends that Bomgar customers should review the Bomgar Appliance Secure Deployment Guide available at: http://www.bomgar.com/docs/content/documents/symantec-secure-deployment.pdf

About Bomgar

Bomgar Corporation's mission is to change the way work is done. Through support virtualization, Bomgar works to free the tech support community from the restraints of access barriers and geography, and from the inefficiency of traditional phone-based and on-site support. Support virtualization makes support more responsive, efficient and secure by removing the geographical and technological barriers between customers and those supporting them.
To learn more about Bomgar, visit them online at: http://www.bomgar.com/

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Mountain View, California, Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our web site. For product information in the U.S., call toll-free at +1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934