Trustwave®
Information Security & Compliance

Bomgar Corporation

Bomgar Application Security Assessment Summary
January 26, 2015

Report Author	John Hoopes Trustwave, SpiderLabs			
Customer	Bomgar Corporation			
Project	Application Security Testing			
Document Control	Draft Version			
Document Control	Revision	0.1	12/18/2014	John Hoopes
	QA Review	0.5	12/19/2014	Trustwave QA
	Final Version	1.0	04/07/2015	John Hoopes

Table of Contents

1 Executive Summary

Bomgar Corporation engaged Trustwave's SpiderLabs to perform a series of Application Penetration Tests of the Bomgar application. The primary objective of this project was to gauge the resiliency of the application to various attacks launched against both authenticated and unauthenticated surfaces. Trustwave conducted the tests between the dates of July 28, 2014 – December 16, 2014.

Trustwave found that the design and implementation of the overall architecture of the Bomgar solution was carried out with security best practices in mind. The observations presented in this document apply to the Bomgar solution running software version 14.2 on all physical and virtual platforms. During testing some issues were identified and remediated during the course of testing. Additional testing was performed to ensure that remediation efforts were effective.

2 Summary of Components Examined

The Bomgar application environment includes the following:

- Bomgar Appliance: The appliance platform can be deployed either as a hardware device or virtual appliance that supports Bomgar's server components and allows administrators to perform configuration tasks. The appliance also provides network connectivity features that allow representatives and customers to communicate in complex environments.
- Bomgar Representative Console: The console is a multi-platform application used by support personnel to access remote customer workstations running the Bomgar Customer Client. The console also provides chat and file transfer functions.
- Bomgar Customer Client: The customer client is an executable that allows support personnel to access the workstation remotely. When the support session is completed, the client can be uninstalled or left in place for future communication.

Areas of interest for the assessment were identified in the early stages of the engagement. The results of this series of tests apply to the Bomgar B200, B300, B400, and Virtual Appliances running Bomgar Software version 14.2 on Bomgar Firmware version 4.0.5. Application testing was divided into the following:

- Bomgar Software Administrative Interface: The administrative interface of the Bomgar application that allows configuration of the product
- Bomgar Firmware Administrative Interface: The administrative interface of the Bomgar firmware and appliance

- Bomgar Jumpoint: An optional executable that extends the unattended functionality of the solution
- Bomgar Jumpoint/vPro: An extensible function of the Jumpoint enabling Intel's vPro access to systems on any network
- Bomgar Representative Console (Windows, Mac, Linux, iOS, Android): A downloaded executable that is used to provide support to an end customer during a support session
- Bomgar Representative Invite: A one-time used Bomgar Representative Console for the purpose of inviting an external representative into a shared support session
- Bomgar Presentation Attendee Client (Windows, iOS, Android): A client used to attend a presentation given by a Bomgar Representative
- Bomgar Customer Client (Windows, Mac, Linux, Blackberry, Windows Mobile, iOS, Android): A downloaded executable that is used to receive support from a representative
- Bomgar Active Jump Client: A persistent Bomgar unattended client installed on an end system that allows for unattended system access by a Bomgar Representative
- Bomgar Passive Jump Client: A non-persistent Bomgar unattended client installed on an end system that allows for unattended system access by a Bomgar Representative
- Bomgar Button: A pre-installed Bomgar Client that can be used by end system user to trigger an initiation of a support session to a Bomgar Representative
- Bomgar Smart Card Support: A capability that enables a representative's smart card to be used in a support session
- Bomgar Connection Agent: An agent that enables secure LDAP connectivity through firewalls
- Bomgar Integration Client: A client that enables information archival from the Bomgar Appliance

3 Testing Environment Description

Trustwave installed all necessary hardware provided by Bomgar. The appliance was installed into an isolated Trustwave testing network so that environmental disruptions were kept to a minimum during the analysis. Also, in order to perform testing on the application components listed in the previous section, base installations of Windows, Linux, iOS, Blackberry, and Android were used. These systems were used to simulate both customers and, in applicable instances, representatives interacting with the central infrastructure.

4 General Observations

The application architecture of Bomgar software implements various security controls that protect both representatives providing support and customers receiving support.

Encryption is enforced and proper authentication ensures that only appropriate users of the system are allowed to manage configuration.

During testing some issues were identified and remediated during the course of testing. Additional testing was performed to ensure that remediation efforts were effective.

Bomgar's efforts, as evidenced by this testing engagement, show a strong basis for a comprehensive information security program. Bomgar has continued a multi-year program of periodic assessments and reviews addressing both technical and policy issues as part of an ongoing information security program.

5 Appliance Deployment Model

The Bomgar application is delivered using a secured appliance model. Management of the appliance is performed using encrypted protocols. The appliance provides a central point for configuration management. It is also mediates all connections between support representatives and clients.

The appliance supports a managed upgrade structure that ensures that the appliance is kept up to date with the latest security technologies.

Trustwave finds that the interfaces available to remote users were restricted to only those requisite for the application to function. Extraneous services had been disabled. Other services were blocked by firewall policy.

6 Secure Communications

Before performing active testing, Trustwave gathered information about how the various elements of the Bomgar application communicates with the appliance. Trustwave manually interacted with the Bomgar clients while monitoring network traffic generated by the client.

Trustwave reviewed Bomgar network traffic to determine if any sensitive communication between the client and server took place using plaintext protocols. Encrypted protocols were reviewed for proper encryption key exchange, mutual endpoint authentication, and certificate signing, as appropriate.

Trustwave finds that Bomgar properly secures all network communications in a way that meets or exceeds industry security best practices.

When possible, Trustwave used tools to analyze the communication protocols used by the Bomgar application. Parts of the communication utilized Bomgar's proprietary protocol therefore manual analysis of the protocol was performed where applicable

during testing. Trustwave identified the various server-side functions called by the client, along with the data passed with each function.

Trustwave finds that the Bomgar application properly designs and implements all network communications with security best practices in mind.

7 Authentication and Authorization

Proper enforcement of authentication was verified for all private areas of the Bomgar application. Tests for authorization bypass by legitimate users were performed – both vertical privilege escalation (such as gaining administrative access) and lateral privileges (performing actions as another user of the same role). When record or object identifiers were specified in user requests, Trustwave modified them to check if unauthorized data could be accessed.

Authentication-related functions such as password-reset functions were also tested. For example, Trustwave attempted to reset passwords using information that an attacker could gain through web searches or other research. Authentication error messages were investigated to determine if they leaked information useful to an attacker. Where relevant, account-creation and password-change pages were tested to see if they could be used to hijack existing accounts.

Trustwave finds that Bomgar implements proper enforcement of authentication and authorization in all private areas of the Bomgar application.

8 Input Validation

Many application vulnerabilities are caused by improper input validation – essentially placing too much trust in the integrity of data provided by users. Specially formatted data can cause the application to behave in unanticipated ways. This can be due to individual meta-characters or longer strings of data. Related vulnerabilities include SQL Injection, XML Entity Expansion, and Buffer Overflows.

When testing for proper input validation, Trustwave probed the Bomgar appliance using data containing non-alphanumeric characters, unusually long character strings, and data in unusual format, and attack strings specific to various technologies. The manner in which the input was provided to the server was highly dependent on the protocol and encoding standards in use. The appliances response to the probes was analyzed to identify any underlying vulnerabilities.

Where possible, Trustwave performed tests using probes known to have special significance within the technologies used by the Bomgar application.

Trustwave found that Bomgar properly sanitized all user-supplied input.