Application Security Assessment
Letter of Attestation

Bomgar Remote Support
Confidential Information

December 18, 2017

Contents

Executive Summary

Overview

Bomgar Corporation (Bomgar) engaged Virtual Security Research, LLC (VSR) to perform a phased series of tests of the Bomgar remote support products. This letter of attestation covers the product penetration assessment of the Bomgar Remote Support appliance targeting the `/login` and `/appliance` endpoints.

The engagement included an in-depth application penetration test of the Bomgar Remote Support solution, in an attempt to identify common web application security vulnerabilities, in addition to those associated with technologies used, implementation, or specific product use cases. The security team evaluated security weaknesses and their potential impact on *Confidentiality*, *Integrity* and *Availability* of the appliance, interaction with the product components, and the data stored within. During testing, the security team found that the design and implementation of the overall architecture of the Bomgar solution was carried out with security best practices in mind.

Upon completion of retesting, the latest version of Bomgar Firmware 5.1 and Software 17.1 were found to have addressed all vulnerabilities with a medium or higher rating.

Scope

The review evaluated the Remote Support web applications used to manage the device and remote support connections.

It is primarily composed of the following components used in physical, virtual, and cloud based deployment models:

- `/appliance` – Application used by administrators to change operating system settings such as networking, storage, and certificates.
- `/login` – Application used by remote support representatives to setup and manage remote connections. Contains many different permission settings.

The testing was concentrated on evaluating the following versions of the Bomgar solution:

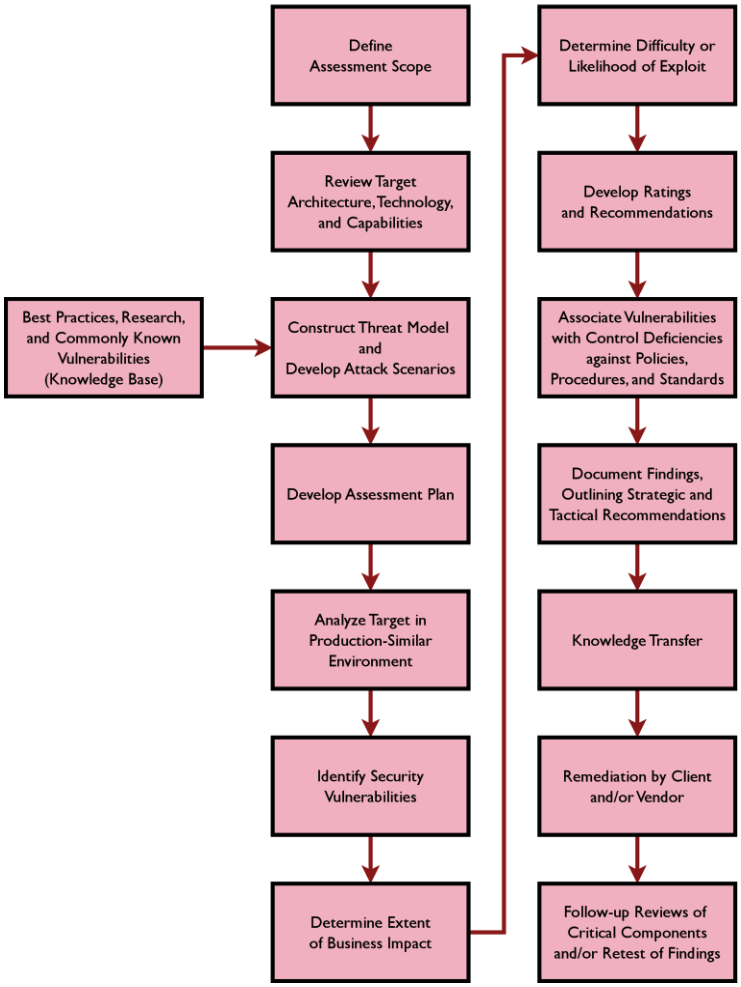
- Firmware: 5.1
- Software: 17.1

Assessment Methodology

An application penetration assessment is designed to highlight potential security vulnerabilities within the application based upon a defined threat model. It is intended to identify design failures and unsafe coding practices, including but not limited to: authentication, authorization, session management, data validation, use of cryptography, error handling, information leakage, and language specific coding issues. During the assessment, VSR has assigned business risk ratings based on our current understanding of the application.

VSR utilizes a comprehensive assessment methodology, providing results with the utmost accuracy and ensuring representational coverage of risks facing an application or information system. This assessment methodology is based upon understanding of the business use cases, types of data stored, processed, or transmitted by a given system or system component. This evaluation involves a form of threat modeling by which system components are broken into their constituent elements representing: use cases, data, users, processes, components, technologies and boundaries. Once these elements are decomposed, potential risks affecting their interaction is evaluated by the assessment team as illustrated by the following process flow:

VSR Attack Simulation Methodology



Application Penetration Assessments

The assessment team relies primarily on manual penetration testing to ensure coverage across OWASP's Top 10 vulnerability classes, as well as other risks resulting from choices in technology, application logic, and integration between application and system components or application use cases.

Our approach and methodology is not limited to OWASP Top 10 vulnerabilities classes, instead allowing the assessment team to adapt testing based upon the risks most likely to affect Bomgar based upon the threat model and attack plan defined during the threat modeling phase of the engagement. The following OWASP Top 10 vulnerability classes are included in each penetration assessment:

- Injection Flaws
- Cross-site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards
- Tools used by VSR during web application penetration tests often include:
  - Burp Proxy
  - WebScarab
  - Zed Attack Proxy
  - w3af
  - sqlmap
  - BeEF
  - Hydra
  - Medusa
  - RainbowCrack
  - John the Ripper
  - SOAPui
  - Nessus
  - Nikto
  - Bletchley
  - Proprietary tools and scripts

The inclusion of manual penetration testing executed during the course of the assessment provides greater coverage over classes of vulnerabilities which often go undetected by automated vulnerability assessment tools, and dynamic web application security scanners. These classes of vulnerabilities which often go undetected by automated only testing solutions include: authentication, authorization, session management, cryptographic weaknesses and application business logic. Lastly, careful manual execution of test cases allows the application security team to identify and closely coordinate test cases that may be more likely to impact system and service availability, thereby minimizing potential impact to production systems.

Common Attack Vectors Considered

During initial preparation for an application security assessment common attack vectors are specified to ensure consistent focus and a comprehensive approach. These provide structure to the engagement team's tasks and are reflected in the final reporting. Some potential attack vectors considered in web-based applications include:

ATTACK VECTORS		
CATEGORY	**TYPICAL VULNERABILITIES**	**AREAS OF INVESTIGATION**
Data Validation	Failure to test the validity of user-supplied data against known parameters, including but not limited to length, character composition, or conformance to a pre-determined syntax.	■ SQL injection ■ Cross-site scripting ■ Form field manipulation ■ Canonicalization ■ Buffer overflows ■ Format string attacks ■ Shell meta-character injection ■ Reliance on client-side security or behavior ■ Miscellaneous input validation issues
Session Management	Failure to use strong, unpredictable session identifiers and to maintain server-stored state such that each request can be uniquely identified and attributed to a certain user.	■ General observations ■ Static session identifiers ■ Easily predictable identifiers ■ Insufficient length ■ Known algorithms ■ Miscellaneous session management issues
Access Controls	Failure to verify the authenticity of a user and enforce appropriate restrictions on certain data or functionality.	■ Authentication bypass ■ Authorization bypass ■ Inconsistent use of access control ■ State manipulation ■ Miscellaneous access control issues
Cryptography	Failure to use strong encryption. This implies using a cryptographically proven algorithm along with a key that is sufficiently random and unpredictable.	■ Proprietary or home-grown encryption ■ Insecure cipher mode ■ Poor key selection ■ Insufficient key length ■ Inappropriate key reuse ■ Miscellaneous cryptography issues
Third-Party Components	Vulnerabilities in supporting architecture that can be remotely exploited to compromise the server or gather useful information.	■ Publicly disclosed vulnerabilities ■ Team proprietary vulnerabilities ■ Configuration errors ■ Default content

About VSR

VSR provides unparalleled security consulting services with a proven methodology and track record for identifying vulnerabilities in business critical systems. Our expertise in penetration techniques and strong knowledge in evolving security trends enables us to effectively identify vulnerabilities in even the most complex systems.

VSR is an expert provider of vendor neutral information and data security assessments as well as advisory services for Fortune 500 clients. The VSR difference is our ability to deliver detailed insight into quantifiable risk. VSR understands that information security comes from the proper mix of people, process and technology and must be tailored to each specific customer.

VSR's primary goal is to provide clients with an unparalleled quality of security consulting services and to maintain our competitive edge through research and innovation.

In November 2016, VSR became part of NCC Group. This strategic acquisition allows us to strengthen our service portfolio through NCC Group to enable us to offer enhanced cyber services worldwide.

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

Headquartered in Manchester, UK, with over 35 offices across the world, NCC Group employs more than 2,000 people and is a trusted advisor to 15,000 clients worldwide.

For more information on VSR, please visit us at: https://www.vsecurity.com/.

For more information about NCC Group, please visit: https://www.nccgroup.trust/uk/.