DARA SECURITY

ADVISORS | ASSESSORS | ETHICAL HACKERS

ezeelogin Secure SSH Gateway

Payment Card Industry Data Security Standard 3.2 Environment Impact Assessment

Company: AdMod Technologies Pvt. Ltd.

Report Date: June 3, 2016

Revision 1.0

Table of Contents

Executive Summary

AdMod Technologies requested that Dara Security, a PCI SSC authorized QSA/PA QSA/P2PE (QSA), perform a functionality and security review of the **ezeelogin** secure SSH gateway solution. ezeelogin is a secure SSH gateway software that helps companies organize, manage and administrate hundreds of Linux servers easily, efficiently and securely. It has automation features like parallel shell, root password management, SSH user management and access control, two factor authentication, one click control panel access, SSH user log recording and more features.

The purpose of the review was to assess the security of the solution and to evaluate its functionality and features to determine if the solution can enable an organization to meet PCI DSS 3.2 requirements for authentication and user access auditing.

Dara Security's responsibility is to express an opinion on the security efficacy of the *ezeelogin* solution based on the technical presentations and documentation provided by AdMod Technologies.

For the PCI DSS 3.2 evaluation, we conducted our examination in accordance with testing standards provided in the PCI DSS v3.2 Audit template published April 2016, on the suitability of the design and operating effectiveness of the *ezeelogin* solution's ability to meet applicable authentication (Requirement 8) and auditing (Requirement 10) requirements. For the security testing, the assessment involved a comprehensive examination of the application layers of AdMod's ezeelogin solution using a white-box testing approach.

The following findings are relevant highlights from this assessment.

- *ezeelogin* integrates securely with any computer supporting ssh as its user access mechanism.
- Security of the *ezeelogin* deployment requires the end-user to follow AdMod Technologies deployment guidelines for the software and underlying supporting architecture.
- When *ezeelogin* is properly deployed, it can securely, centrally manage authentication for enabled devices and systems.
- *ezeelogin* does enable an organization to meet PCI DSS 3.2 requirements for authentication and user access auditing for managed systems.
- Security testing of the solution confirmed that, during the time frame of the testing, the software does not introduce any security vulnerabilities when properly performed.

This white paper has two target audiences:

- Organizations interested in a centralized authentication management solution and its impact to the environment.
- The QSA and Internal Audit community that is evaluating a deployment of ezeelogin with an organization’s environment.

About PCI DSS 3.2

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and to facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI DSS comprises a minimum set of requirements for protecting account data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with applicable PCI DSS requirements. PCI DSS requirements apply to organizations where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted.

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the third party protects the account data, per the applicable PCI DSS requirements.

Evaluation Assessment Scope

The objective of the engagement was two-fold. First, it evaluated the security of the ezeelogin solution itself to determine if the solution would introduce vulnerabilities into an organization's environment. The second goal of the assessment was to demonstrate if the solution can enable an organization to meet PCI DSS 3.2 requirements for authentication and user access auditing.

For the testing and evaluation, certain assumptions were made:

- The application is deployed in a manner dictated by AdMod Technologies deployment guides;
- Deployment of the supporting infrastructure would be performed in a manner consistent with securing of a PCI DSS in-scope environment to include:
    - Current patching of supporting systems operating the ezeelogin software;
    - Disablement of SSLv3 and early TLS per PCI DSS requirements for web server software presenting the ezeelogin web interface; and
    - Configuration hardening and disablement of web server features to eliminate security flaws within the web server software presenting the ezeelogin web interface.

Security Assessment Evaluation

Using industry best practices in its assessment and testing methodologies, including standard audit methods, Dara Security conducted technical lab testing on the *ezeelogin* solution. This assessment involved a comprehensive examination of the application layers of AdMod's ezeelogin solution. AdMod requested a white box-testing scenario, with a clear, defined scope available to analysts at the time of testing. Our examination involved performing procedures to obtain evidence about the security efficacy of the technical presentation and documentation on the *ezeelogin* solution.

Tools Used

Dara Security uses a variety of commercial and public tools, as well as public and proprietary scripts, depending on the services and operating systems identified throughout the assessment. Additionally, specific findings may have their own scripts to verify and successfully exploit a vulnerability. Due to unique environments from one test to the next, and with the constant changes in technology and protocols, a current list of tools is provided on Dara's website at the following URL.

https://www.darasecurity.com/resources/tools.php

True penetration testing requires the ingenuity of human interaction and manipulation, with tools only aiding in a limited fashion. Dara Security uses Qualys and Nessus as its two primary vulnerability scanning tools. A variety of operating systems are used to scan, attack and exploit targets, including popular penetration testing distributions, such as Kali Linux and Samurai WTF. Identification and confirmation of vulnerabilities is performed with the use of additional tools and scripts as well as by hand.

Methodology

The approach to a penetration test can vary depending on the needs of a particular client. Black box testing, sometimes referred to as double blind testing, refers to testing with no prior knowledge of the company's network environment. Usually analysts only have a company name to begin and must next identify registered and leased IP address ranges. Testing proceeds with the assistance of the client to ensure incorrect IP addresses are not targeted. Black box testing is often selected to test with the mindset of an outside attacker who has no knowledge of the target environment whatsoever.

The opposite of black box testing is white box. White box testing refers to analysts approaching the pentest with knowledge that an outsider would not normally have. This typically applies to testing an inside threat - what a rogue employee or intruder with privileged information could do to the target company. Some examples of information that may be shared with analysts in white box testing include network diagrams, login credentials, remote access credentials, internal IP addressing scheme, source code and access to key personnel.

Dara Security prefers to approach the assessment as a white box penetration test. It is not Dara Security's policy to knowingly trigger a vulnerability or condition that would result in a denial of service. A denial of service, or DoS, is an attempt to make a host or service unusable by means of flooding the target with requests until it is rendered inoperable to legitimate users. Instead, these issues will be presented within the report, but will require AdMod to investigate further.

Dara Security has developed a customized penetration testing methodology based heavily on the Open Source Security Testing Methodology Manual (OSSTMM), which is freely available at http://www.isecom.org/. The OSSTMM provides a scientific methodology to ensure consistent, reliable results, applicable to any technical audit type. Dara Security analysts ensured testing was conducted thoroughly, complied with any applicable laws, was measurable in a quantifiable matter, was consistent and repeatable and that the report only contained facts as derived from the assessment.

Security Assessment Results

Security testing of the solution and its supporting environment found no security issues within the software and environment when deployed in a manner consistent with documentation provided by AdMod Technologies for use of the ezeelogin solution. Monitoring of authentication communication between the ezeelogin solution and management devices confirmed that authentication communications are encrypted and secured in transit.

No vulnerabilities were discovered during this process.

Environment PCI DSS Authentication and Auditing Impact

There will always be certain controls for PCI DSS compliance that must be independently assessed in any environment. PCI DSS compliance will always apply to an environment that transmits, processes or stores cardholder data anywhere in its physical environment. By properly implementing the AdMod Technologies ezeelogin solution, an organization can effectively manage disparate systems that utilize SSH for authentication and access.

The following sections and corresponding charts provide Dara Security's opinion of which requirements the ezeelogin solution supports.

PCI DSS 3.2 Impact Detail by Applicable Requirement

If a specific requirement is not listed, then that requirement is not impacted by the solution.

PCI DSS 3.2 Requirement 8: Identify and authenticate access to system components	
PCI DSS Requirement	**Description of Requirement Impact**

8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:
• **8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data.
• **8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
• **8.1.3** Immediately revoke access for any terminated users.
• **8.1.4** Remove/disable inactive user accounts within 90 days.
• **8.1.5** Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:
  ○ Enabled only during the time period needed and disabled when not in use.
  ○ Monitored when in use.
• **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts.
• **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
• **8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.

PCI DSS 3.2 Requirement 8: Identify and authenticate access to system components	
PCI DSS Requirement	**Description of Requirement Impact**
• Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric.	
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	The ezeelogin solution supports the use of strong cryptography for the storage of authentication credentials. It is the responsibility of the end-user organization to properly configure SSH and HTTPS to disallow the use of SSLv3 and early TLS.
8.2.2 Verify user identity before modifying any authentication credential —for example, performing password resets, provisioning new tokens, or generating new keys.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.
8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.
8.2.4 Change user passwords/passphrases at least once every 90 days.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication **Note:** Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of	The ezeelogin solution supports the enforcement of defined user identification and multi-factor authentication controls. It is the responsibility of the end-user to implement proper management procedures.

PCI DSS 3.2 Requirement 8: Identify and authenticate access to system components	
PCI DSS Requirement	**Description of Requirement Impact**
authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials. • Guidance for how users should protect their authentication credentials. • Instructions not to reuse previously used passwords. • Instructions to change passwords if there is any suspicion the password could be compromised.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	The ezeelogin solution supports the enforcement of defined user identification and authentication controls. It is the responsibility of the end-user to implement proper management procedures.

PCI DSS 3.1 Requirement 10: Track and monitor all access to network resources and cardholder data	
PCI DSS Requirement	**Description of Requirement Impact**
10.1 Implement audit trails to link all access to system components to each individual user.	The ezeelogin solution supports the enforcement of user access audit controls for access to the ezeelogin solution and to devices for which is manages authentication. It is the responsibility of the end-user to implement proper management procedures.
10.2 Implement automated audit trails for all system components to reconstruct the following events: • **10.2.1** All individual user accesses to cardholder data. • **10.2.2** All actions taken by any individual with root or administrative privileges. • **10.2.3** Access to all audit trails. • **10.2.4** Invalid logical access attempts. • **10.2.5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. • **10.2.6** Initialization, stopping, or pausing of the audit logs. • **10.2.7** Creation and deletion of system-level objects.	The ezeelogin solution supports the enforcement of user access audit controls for access to the ezeelogin solution and to devices for which is manages authentication. It is the responsibility of the end-user to implement proper management procedures.
10.3 Record at least the following audit trail entries for all system components for each event: • **10.3.1** User identification • **10.3.2** Type of event • **10.3.3** Date and time • **10.3.4** Success or failure indication • **10.3.5** Origination of event • **10.3.6** Identity or name of affected data, system component, or resource	The ezeelogin solution supports the enforcement of user access audit controls for access to the ezeelogin solution and to devices for which is manages authentication. It is the responsibility of the end-user to implement proper management procedures.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing	The ezeelogin system is capable of time synchronization with an organizations NTP deployment.

PCI DSS 3.1 Requirement 10: Track and monitor all access to network resources and cardholder data	
PCI DSS Requirement	**Description of Requirement Impact**
time. • **10.4.1** Critical systems have the correct and consistent time. • **10.4.2** Time data is protected. • **10.4.3** Time settings are received from industry-accepted time sources.	
10.5 Secure audit trails so they cannot be altered. • **10.5.1** Limit viewing of audit trails to those with a job-related need. • **10.5.2** Protect audit trail files from unauthorized modifications. • **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. • **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. • **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	The ezeelogin solution supports the enforcement of user access audit controls for access to the ezeelogin solution and to devices for which is manages authentication. It is the responsibility of the end-user to implement proper management procedures.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. • **10.6.1** Review the following at least daily: 1. All security events 2. Logs of all system components that store, process, or transmit CHD and/or SAD 3. Logs of all critical system components 4. Logs of all servers and system components that perform security functions (for example, firewalls,	The ezeelogin system is capable of retaining logs and sending logs to a defined centralized logging server. It is the responsibility of the end-user to implement proper management procedures.

PCI DSS 3.1 Requirement 10: Track and monitor all access to network resources and cardholder data	
PCI DSS Requirement	**Description of Requirement Impact**
intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). • **10.6.2** Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. • **10.6.3** Follow up exceptions and anomalies identified during the review process.	
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	The ezeelogin system is capable of retaining logs and sending logs to a defined centralized logging server. It is the responsibility of the end-user to implement proper management procedures.