SUMMARY

PCI ASV Report

ALERT LOGIC™

ALERT LOGIC™

PCI ASV REPORT

Attestation of Scan Compliance

Overall summary of compliance status, and assertion of the scan scope and that the scan complies with PCI requirements.

Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, ISO 27001-2013, and ISO/IEC 27701:2019 certification for UK Operations.

PCI ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	Albert Systems			Company:	Alert Logic, Inc. (4222-01-11)		
Contact:	John Doe	Title:		Contact:	Robert LaBlah	Title:	Team Lead, Compliance Specialists
Telephone:	(555) 555-5555	E-mail:	john.doe@albertsystems.com	Telephone:	(713) 351-1776	E-mail:	support@alertlogic.com
Business Address:				Business Address:	1776 Yorktown - 7th Floor		
City:		State / Province:		City:	Houston	State / Province:	TX
ZIP:		URL:		ZIP:	77056	URL:	http://www.alertlogic.com

A.3 Scan Status			
Date scan completed:	October 1, 2017 11:35am	Scan expiration date (90 days from date scan completed):	January 1, 2018
Compliance Status:	Fail	Scan report type:	[*] Full scan [ ] Partial scan or rescan
Number of unique components* scanned:	1		
Number of identified failing vulnerabilities:	4		
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope:	0		

* A component includes any host, virtual host, IP address, domain, FQDN or unique vector into a system or cardholder data environment.

A.4 Scan Customer Attestation

Albert Systems attests on October 1, 2017 11:35am that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions-including compensating controls if applicableâ€”is accurate and complete. Albert Systems also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Alert Logic under certificate number 4222-01-11, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.
Alert Logic attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Robert LaBlah.

PCI ASV REPORT

Executive Summary

Overview of scan results and a statement of compliance or non-compliance.

Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, ISO 27001-2013, and ISO/IEC 27701:2019 certification for UK Operations.

PCI ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information

Company:	Albert Systems		
Contact:	John Doe	Title:	
Telephone:	(555) 555-5555	E-mail:	john.doe@albertsystems.com
Business Address:			
City:		State / Province:	
ZIP:		URL:	

A.2 Approved Scanning Vendor Information

Company:	Alert Logic, Inc. (4222-01-11)		
Contact:	Robert LaBlah	Title:	Team Lead, Compliance Specialists
Telephone:	(877) 960-3383	E-mail:	support@alertlogic.com
Business Address:	1776 Yorktown - 7th Floor		
City:	Houston	State / Province:	TX
ZIP:	77056	URL:	http://www.alertlogic.com

A.3 Scan Status

Date scan completed:	October 1, 2017 11:35am	Scan expiration date (90 days from date scan completed):	January 1, 2018
Compliance Status:	Fail	Scan report type:	[*] Full scan [ ] Partial scan or rescan
Number of unique components* scanned:	1		
Number of identified failing vulnerabilities:	4		
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope:	0		

* A component includes any host, virtual host, IP address, domain, FQDN or unique vector into a system or cardholder data environment.

A.4 Scan Customer Attestation

Albert Systems attests on Octobery 1, 2017 11:35am that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions-including compensating controls if applicableâ€”is accurate and complete. Albert Systems also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Alert Logic under certificate number 4222-01-11, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.
Alert Logic attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Robert LaBlah.

PCI ASV Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	Albert Systems	ASV Company:	Alert Logic, Inc. (4222-01-11)
Date scan was completed:	October 1, 2017 11:35am	Scan expiration date:	January 1, 2018

Part 1.a Submitted Scan Scope

178.62.7.32

Part 2. Component Compliance Summary

Components (IP Address, domain, etc.):	178.62.7.32	Fail

Part 3a. Vulnerabilities Noted for each Component

178.62.7.32

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
178.62.7.32 Port: 80/tcp	Clickjacking - X-Frame-Options Header missing	Medium	6.8	Fail	No NIST CVSS base score is available; exposure rated by vendor (fail)
178.62.7.32 Port: 80/tcp	Autocomplete Password in Browser	Medium	6.2	Fail	No NIST CVSS base score is available; exposure rated by vendor (fail)
178.62.7.32 Port: 22/tcp	CVE-2016-0778 - OpenSSH - Buffer Overflow Issue	Medium	4.6	Fail	
178.62.7.32 Port: 22/tcp	CVE-2016-0777 - OpenSSH - Information Disclosure Issue	Medium	4.0	Fail	
178.62.7.32 Port: 443/tcp	Web Service is Running	Low	2.1	Pass	No NIST CVSS base score is available; exposure rated by vendor (pass)
178.62.7.32 Port: 80/tcp	Web Service is Running	Low	2.1	Pass	No NIST CVSS base score is available; exposure rated by vendor (pass)
178.62.7.32	TCP Timestamp	Low	0.0	Pass	Informational only.

Consolidated Solution/Correction Plan for above Component:

- Reconfigure Service to be More Secure
- Upgrade OpenBSD OpenSSH to version 7.2.0
- Disable or Uninstall Unused Software

Part 3b. Special notes by Component

Component	Special Note	Item Noted	Scan customer's description of action taken and declaration that software is either implemented securely or removed
178.62.7.32	Due to increased risk to the cardholder data environment when remote access software is present, ...	Remote Access - ssh - Port:22	

Part 3c. Special notes - Full text

Note
Remote Access - ssh - Port:22 Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.

Part 4a. Scan Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.
178.62.7.32

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.
178.62.7.32

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

ALERT LOGIC™

PCI ASV REPORT

Vulnerability Details Summary

Detailed description, impacted hosts, risk level, and remediation guidance for each vulnerability.

PCI DSS COMPLIANT

AICPA SOC 2

ISO 27001 CERTIFIED A-LIGN

Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, ISO 27001-2013, and ISO/IEC 27701:2019 certification for UK Operations.

ALERT LOGIC™

PCI ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	Albert Systems			Company:	Alert Logic, Inc. (4222-01-11)		
Contact:	John Doe	Title:		Contact:	Robert LaBlah	Title:	Team Lead, Compliance Specialists
Telephone:	(555) 555-5555	E-mail:	john.doe@albertsystems.com	Telephone:	(713) 351-1776	E-mail:	support@alertlogic.com
Business Address:				Business Address:	1776 Yorktown - 7th Floor		
City:		State / Province:		City:	Houston	State / Province:	TX
ZIP:		URL:		ZIP:	77056	URL:	http://www.alertlogic.com

A.3 Scan Status			
Date scan completed:	October 1, 2017 11:35am	Scan expiration date (90 days from date scan completed):	January 1, 2018
Compliance Status:	Fail	Scan report type:	[*] Full scan [ ] Partial scan or rescan
Number of unique components* scanned:	1		
Number of identified failing vulnerabilities:	4		
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope:	0		
* A component includes any host, virtual host, IP address, domain, FQDN or unique vector into a system or cardholder data environment.			

A.4 Scan Customer Attestation

Albert Customer attests on Oct 1, 2017 11:35am that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions-including compensating controls if applicableâ€”is accurate and complete. Albert Systems also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Alert Logic under certificate number 4222-01-11, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.
Alert Logic attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Robert LaBlah.

PCI Scan Report Vulnerability Details

Part 1. Scan Information			
Scan Customer Company:	Albert Systems	ASV Company:	Alert Logic, Inc. (4222-01-11)
Date scan was completed:	October 1, 2017 11:35am	Scan expiration date:	March 1, 2018

Part 2. Vulnerability Details

IP: 221.99.1.53	No CVE assigned	**Name:** TCP Timestamp **Action:** Disable or Uninstall Unused Software	**PCI:** Pass
Hostname:		**Pass/Fail Reason:** Informational only.	
Service: UNKNOWN		**CVSS:** 0.0 - Low - (AV:N/AC:M/Au:N/C:N/I:N/A:N/E:ND/RL:ND/RC:ND)	**EID:** 1080
Description: TCP timestamps are meant to protect against sequence numbers that have surpassed their original 32-bit cap and have "wrapped." These timestamps are generated with a seed value and incremented at a regular interval.			
Evidence: TCP Timestamp			
Impact: If the seed value is known (for example: 0), timestamps can be used to calculate system uptime and boot time. This information can further reveal system information about hardware and software being used, as well as help link spoofed IP and MAC addresses.			
Solution: Check with your vendor for the option to disable TCP timestamps.			
References: http://uptime.netcraft.com http://www.forensicswiki.org/wiki/TCP_timestamps http://www.ietf.org/rfc/rfc1323.txt			

IP: 221.99.1.53 **Port:** 22/tcp	CVE-2016-0778	**Name:** CVE-2016-0778 - OpenSSH - Buffer Overflow Issue **Action:** Upgrade OpenBSD OpenSSH to version 7.2.0	**PCI:** Fail
Hostname:		**Pass/Fail Reason:**	
Service: SSH		**CVSS:** 4.6 - Medium - (AV:N/AC:H/Au:S/C:P/I:P/A:P/E:F/RL:OF/RC:C)	**EID:** 87207
Description: OpenSSH is an open-source implementation of the SSH protocol. A buffer overflow vulnerability has been discovered in OpenSSH, when certain proxy and forward options are enabled. This vulnerability could allow an attacker to cause denial-of-service conditions.			
Evidence: SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3			
Impact: This application is prone to this vulnerability because of a boundary condition error, allowing an attacker to cause denial-of-service conditions.			
Solution: It is recommended that users upgrade to the latest version of OpenSSH. This vulnerability has been fixed in OpenSSH 7.1p2.			
References: http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10734 http://lists.apple.com/archives/security-announce/2016/Mar/msg00004.html http://www.openssh.com/txt/release-7.1p2 http://www.openwall.com/lists/oss-security/2016/01/14/7 http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html http://www.securityfocus.com/bid/80698 https://blogs.sophos.com/2016/02/17/utm-up2date-9-354-released/ https://blogs.sophos.com/2016/02/29/utm-up2date-9-319-released/ https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05247375 https://support.apple.com/HT206167 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0778			

IP: 221.99.1.53 **Port:** 22/tcp	CVE-2016-0777	**Name:** CVE-2016-0777 - OpenSSH - Information Disclosure Issue **Action:** Upgrade OpenBSD OpenSSH to version 7.2.0	**PCI:** Fail
Hostname:		**Pass/Fail Reason:**	
Service: SSH		**CVSS:** 4.0 - Medium - (AV:N/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C)	**EID:** 87206
Description: OpenSSH is an open-source implementation of the SSH protocol. An information disclosure vulnerability has been discovered in OpenSSH. This vulnerability could allow an attacker to obtain sensitive information from process memory.			
Evidence: SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3			
Impact: This application is prone to this vulnerability because of an unknown error, allowing an attacker to obtain sensitive information from process memory.			

Part 2. Vulnerability Details

Solution: It is recommended that users upgrade to the latest version of OpenSSH. This vulnerability has been fixed in OpenSSH 7.1p2.

It is recommended that Red Hat users apply the following workaround to fix this vulnerability:

In Red Hat Enterprise Linux 7 you can mitigate this issue by setting the following option in the OpenSSH client's configuration file, either global (/etc/ssh/ssh_config) or user specific (~/.ssh/config):

```
UseRoaming no
```

The above directive should be placed in the Host * section of the configuration file to use this setting for all SSH servers the client connects to.

You can also set the option via a command line argument when connecting to an SSH server:

```
-o 'UseRoaming no'
```

References:
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10734
http://lists.apple.com/archives/security-announce/2016/Mar/msg00004.html
http://www.openssh.com/txt/release-7.1p2
http://www.openwall.com/lists/oss-security/2016/01/14/7
http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
http://www.securityfocus.com/bid/80695
https://blogs.sophos.com/2016/02/17/utm-up2date-9-354-released/
https://blogs.sophos.com/2016/02/29/utm-up2date-9-319-released/
https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05247375
https://support.apple.com/HT206167
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0777

IP: 221.99.1.53 **Port:** 80/tcp	No CVE assigned	**Name:** Clickjacking - X-Frame-Options Header missing **Action:** Reconfigure Service to be More Secure	**PCI:** Fail
Hostname:		**Pass/Fail Reason:** No NIST CVSS base score is available; exposure rated by vendor (fail)	
Service: HTTP		**CVSS:** 6.8 - Medium - (AV:N/AC:M/Au:N/C:P/I:P/A:P/E:H/RL:ND/RC:C)	**EID:** 81912

Description: The X-Frame-Options HTTP header field declares a policy, communicated from the server to the client browser, regarding whether the browser may display the transmitted content in frames that are part of other web pages. A clickjacking vulnerability has been discovered when the X-Frame-Options Header is not set. This vulnerability could allow an attacker to disclose information or redirect users.

Evidence: Web Server, No details are available.

Impact: Web applications are prone to this vulnerability because of websites allowing framing from other domains, allowing an attacker to disclose information or redirect users.

Solution: It is recommended that users send the proper X-Frame-Options HTTP response headers that instruct the browser to not allow framing from other domains.

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options
https://www.owasp.org/index.php/Clickjacking
https://cwe.mitre.org/data/definitions/693.html

IP: 221.99.1.53 **Port:** 80/tcp	No CVE assigned	**Name:** Autocomplete Password in Browser **Action:** Reconfigure Service to be More Secure	**PCI:** Fail
Hostname:		**Pass/Fail Reason:** No NIST CVSS base score is available; exposure rated by vendor (fail)	
Service: HTTP		**CVSS:** 6.2 - Medium - (AV:L/AC:L/Au:S/C:C/I:C/A:N/E:F/RL:W/RC:C)	**EID:** 25962

Description: The HTML application was found to contain a Username and Password box that does not explicitly disable the use of the web browsers password autocomplete function, this is considered unsafe and should be corrected.

Evidence: /, Password type input named <b><font color="dark">pwd</font></b> from <b>unnamed form</b> with action <b>login.php</b> has autocomplete enabled.

Impact: The password autocomplete should always be disabled, especially in sensitive applications, since an attacker, if able to access the browser cache, could obtain the password in cleartext (public computers are a very notable example of this attack).

Solution: Check the HTML code of the login page to see whether browser caching of the passwords is disabled. The code for this will usually be along the following lines:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

The "remember my password" mechanism can be implemented with one of the following methods:

Allowing the "cache password" feature in web browsers. As of 2014 this is the preferred method as all major browsers have disabled the setting of autocomplete="off" by default for password fields.
Storing the password in a permanent cookie. The password must be hashed/encrypted and not sent in the clear.

References:
http://www.owasp.org/index.php/Testing_for_Vulnerable_Remember_Password_and_Pwd_Reset
http://www.owasp.org/index.php/Guide_to_Authentication#Browser_remembers_passwords
https://www.owasp.org/index.php/Testing_for_Vulnerable_Remember_Password_(OTG-AUTHN-005)
https://developer.mozilla.org/en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion

IP: 221.99.1.53 **Port:** 80/tcp	No CVE assigned	**Name:** Web Service is Running **Action:** Disable or Uninstall Unused Software	**PCI:** Pass

Part 2. Vulnerability Details

Hostname:		**Pass/Fail Reason:** No NIST CVSS base score is available; exposure rated by vendor (pass)	
Service: HTTP	**CVSS:** 2.1 - Low - (AV:L/AC:L/Au:N/C:P/I:N/A:N/E:ND/RL:ND/RC:ND)		**EID:** 11438
Description: A web server is running on this port.			
Evidence: Port: 80, Microsoft-HTTPAPI/2.0			
Impact: There are many vulnerabilities that have been found with all versions of web servers.			
Solution: If the web services on a machine are not essential then they should be removed.			
References:			

IP: 221.99.1.53 **Port:** 443/tcp	No CVE assigned	**Name:** Web Service is Running **Action:** Disable or Uninstall Unused Software	**PCI:** Pass
Hostname:		**Pass/Fail Reason:** No NIST CVSS base score is available; exposure rated by vendor (pass)	
Service: HTTP	**CVSS:** 2.1 - Low - (AV:L/AC:L/Au:N/C:P/I:N/A:N/E:ND/RL:ND/RC:ND)		**EID:** 11438
Description: A web server is running on this port.			
Evidence: Port: 443, Microsoft-HTTPAPI/2.0			
Impact: There are many vulnerabilities that have been found with all versions of web servers.			
Solution: If the web services on a machine are not essential then they should be removed.			
References:			

Part 3. Detailed Profile Information

221.99.1.53		
OS	Linux Linux 3.X	
unknown	0	tcp
ssh	22	tcp
http	80	tcp
http	443	tcp