Security Settings Audit

FORTRA

Generated On	08/22/23 4:53:29 PM
Organization	Sample
Environment	Sample
Passed	33
Warning	4
Failed	45
Fatal	1
Not Applicable	0

Security Check	Status	Recommendation	PCI DSS Section
GoAnywhere Gateway is enabled to provide a reverse proxy service for inbound connections.	Failed	Install GoAnywhere Gateway in the DMZ, which will allow ports to be closed into the private network and keep sensitive files out of the DMZ. Ensure that GoAnywhere MFT is installed in the private (internal) network.	1.2.1, 1.3.2, 1.3.6, 1.3.7
The default Admin User 'administrator' is disabled or is not using the default password.	Failed	Disable the default 'administrator' Admin User account or change its password to a different value than the default.	2.1
The default Admin User 'root' is disabled or is not using the default password.	Failed	Disable the default 'root' Admin User account or change its password to a different value than the default.	2.1
The default certificate is not used by the HTTPS admin server.	Passed		2.1
The default certificate is not used by the HTTPS/AS2/AS4 service.	Passed		2.1
The default certificate is not used by the FTP service.	Passed		2.1
The default certificate is not used by the FTPS service.	Passed		2.1
The default SSH host keys are not used by the SFTP service.	Passed		2.1
The SFTP service software version, which is shown after user login, does not contain the default string of "GoAnywhere".	Failed	The Software Version for the SFTP service is not specified. Within the Service Manager, specify a value for the Software Version for the SFTP service to show after login. The Software Version should not be left blank or show the word "GoAnywhere".	2.1
GoAnywhere application is separate from the database server.	Passed		2.2.1
The HTTPS/AS2/AS4 service does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Passed		2.2.2, 2.2.3, 4.1
The HTTPS admin server does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Failed	Within the Admin Server Configuration, the following HTTP listeners should be disabled or redirection should be configured to a secure HTTPS listener: 'default' 'default'	2.2.2, 2.2.3, 2.3, 4.1
The control channel between GoAnywhere MFT and GoAnywhere Gateway is encrypted using SSL/TLS.	Failed	Enable SSL in the Control Channel Security section of the Gateway Configuration screen in GoAnywhere MFT. You must also enable SSL in the Gateway software installation.	2.2.3

Security Check	Status	Recommendation	PCI DSS Section
A Shared Secret is used to establish trust between GoAnywhere MFT and GoAnywhere Gateway.	Passed		2.2.3
The HTTPS admin server does not allow outdated versions of SSL or TLS protocols.	Failed	Within the Admin Server Configuration, the following HTTPS admin listeners should be configured to only allow SSL protocol versions TLSv1.1 and TLSv1.2: 'secured' 'secured'	2.2.3, 2.3, 4.1
The HTTPS/AS2/AS4 service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.3, 4.1
FTP protocol is not allowed for inbound connections unless it is encrypted.	Failed	Standard FTP is enabled and Explicit SSL encryption is not specified for the following FTP listeners: 'default' 'default' Within the Service Manager, the FTP server should be disabled or Explicit SSL should be enforced by enabling the 'Force Encrypted Authentication' and 'Force Encrypted Data Channels' settings for the FTP Server.	2.2.2, 2.2.3, 4.1
Explicit SSL on the FTP service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.3, 4.1
The FTPS service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.3, 4.1
Secure Mail passwords are not included in the primary email notification.	Failed	In the Secure Mail Settings, disable the ability to include passwords in email notifications or require that those passwords are sent in a separate email.	2.2.4
Do not allow browsers to save login credentials for Admin Users.	Failed	Within the Admin Security Settings, disable the 'Allow Browsers to Save Login Credentials' setting.	2.2.4
Do not allow browsers to save login credentials for Web Users.	Failed	Within the Service Manager, disable the 'Allow Browsers to Save Login Credentials' for the HTTPS Web Client.	2.2.4
Administrators with the Resource Manager role are not allowed to view passwords on Resources.	Failed	Disable the 'Allow Viewing of Resource Passwords' setting in the Admin Security Settings.	2.2.4
An overall disk quota is specified for GoDrive.	Passed		3.1
Encrypted folders are configured in GoAnywhere.	Passed		3.4
The Key Manager role is restricted to a small number of Admin Users that can create/manage keys and certificates.	Warning	More than 2 Admin Users have authority to the Key Manager role. It is recommended to restrict this role to essential Admin Users.	3.5.2, 7.1
All certificates are current.	Fatal		3.6.5
All PGP keys are current.	Passed		3.6.5
Only FIPS 140-2 validated encryption ciphers are used for SSL and SSH channels, which is applicable to FTPS, HTTPS, AS2, AS4, SFTP and SCP protocols.	Warning	Enable the FIPS 140-2 Compliance mode to use only validated and strong cipher algorithms for SSL and SSH channels.	4.1

Security Check	Status	Recommendation	PCI DSS Section
The HTTPS admin server uses only the strong ciphers of AES and TDES (3DES).	Passed		4.1
The HTTPS/AS2/AS4 service uses only the strong ciphers of AES and TDES (3DES).	Failed	Configure the following HTTP/AS2/AS4 listeners to only select cipher suites that use AES or 3DES algorithms: 'default' 'default' All other cipher suites should be disabled. This can be configured in the Service Manager.	4.1
Explicit SSL on the FTP service uses only the strong ciphers of AES and TDES (3DES).	Failed	Configure the following FTP listeners to only select cipher suites that use AES or 3DES algorithms: 'default' 'default' All other cipher suites should be disabled. This can be configured in the Service Manager.	4.1
The FTPS service uses only the strong ciphers of AES and TDES (3DES).	Failed	Configure the following FTPS listeners to only select cipher suites that use AES or 3DES algorithms: 'default' 'default' All other cipher suites should be disabled. This can be configured in the Service Manager.	4.1
The SFTP service uses only the strong ciphers of AES and TDES (3DES).	Failed	Configure the SFTP service to only select the cipher algorithms of AES and 3DES. All other cipher algorithms should be disabled. This is configured in the Service Manager.	4.1
The HTTPS admin server does not use outdated Mac Algorithms.	Passed		4.1
The HTTPS/AS2/AS4 service does not use outdated Mac Algorithms.	Failed	Configure the following HTTP/AS2/AS4 listeners to only select cipher suites that do not use the MD5 Mac Algorithm: 'default' 'default' This can be configured in the Service Manager.	4.1
Explicit SSL on the FTP service does not use outdated Mac Algorithms.	Failed	Configure the following FTP listeners to only select cipher suites that do not use the MD5 Mac Algorithm: 'default' 'default' This can be configured in the Service Manager.	4.1
The FTPS service does not use outdated Mac Algorithms.	Failed	Configure the following FTPS listeners to only select cipher suites that do not use the MD5 Mac Algorithm: 'default' 'default' This can be configured in the Service Manager.	4.1
The HTTPS admin server does not use weak Diffie Hellman key exchange algorithms.	Warning	The Diffie Hellman key exchange should only be used if the key size is larger than 1024 bits. Verify your JRE is configured to use 2048 bit DH keys, or configure the following HTTPS Admin listeners to only select cipher suites that do not use the Diffie Hellman key exchange algorithms: 'secured' 'secured'	4.1

Security Check	Status	Recommendation	PCI DSS Section
		This can be configured in the Admin Server Configuration.	
The HTTPS/AS2/AS4 service does not use weak Diffie Hellman key exchange algorithms.	Failed	Configure the following HTTP/AS2/AS4 listeners to only select cipher suites that do not use the Diffie Hellman Export key exchange algorithms: 'default' 'default' This can be configured in the Service Manager.	4.1
Explicit SSL on the FTP service does not use weak Diffie Hellman key exchange algorithms.	Failed	Configure the following FTP listeners to only select cipher suites that do not use the Diffie Hellman Export key exchange algorithms: 'default' 'default' This can be configured in the Service Manager.	4.1
The FTPS service does not use weak Diffie Hellman key exchange algorithms.	Failed	Configure the following FTPS listeners to only select cipher suites that do not use the Diffie Hellman Export key exchange algorithms: 'default' 'default' This can be configured in the Service Manager.	4.1
The SFTP service does not use outdated Mac Algorithms.	Failed	Configure the SFTP service to disable the 'hmac-md5' mac algorithm. This is configured in the Service Manager.	4.1
GoAnywhere product software was updated within the last 6 months.	Passed		6.2
Java Runtime Environment (JRE) for the GoAnywhere product is at version 1.8 or higher.	Passed		6.2
HTTPS Web Client does not allow embedding within an IFrame.	Passed		6.5.7, 6.6
HTTPS Web Client does not allow the Session ID to be stored in the URL.	Passed		6.5.10, 6.6
Brute Force Attacks are monitored and blocked with IP auto-blocking.	Passed		6.6
Denial-of-Service (DoS) Attacks are monitored and blocked with IP auto-blocking.	Failed	Enable the DoS Attack Monitor in the Automatic IP Block List feature.	6.6
IP Filtering is enabled to be performed in the GoAnywhere Gateway.	Warning	Enable the 'Gateway IP Filter' setting in the Gateway Manager.	6.6
Restrict the role of Security Officer (the highest level of authority) to a small number of Admin Users.	Failed	More than 2 Admin Users have authority to the Security Officer role, which can be used to access all administrator features in GoAnywhere. It is recommended to restrict this role to essential Admin Users.	7.1
All Admin User accounts have been active within the last 90 days.	Failed	20 Admin User accounts are enabled and have not logged in within the last 90 days. These accounts should be disabled or deleted.	8.1.4
All Web User accounts have been active within the last 90 days.	Passed		8.1.4
Web Users are automatically disabled when no activity for 90 days.	Passed		8.1.4
Web User accounts are disabled after no more than 6 login failures.	Failed	In the Web User Settings, change the 'Disable Web User Accounts After' setting to 6 attempts	8.1.6, 8.1.7

Security Check	Status	Recommendation	PCI DSS Section
		or less.	
The HTTPS admin server requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The HTTPS/AS2/AS4 service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Failed	Change the HTTPS general preference of 'Session Timeout' to 900 seconds or less in the Service Manager.	8.1.8
The FTP service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The FTPS service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The SFTP service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The default AS2 service settings require trading partner authentication or signatures for inbound AS2 messages.	Passed		8.2
All AS2 Web User accounts require authentication or signatures for inbound AS2 messages.	Passed		8.2
Minimum password length for Admin Users is at least 7 characters.	Passed		8.2.3
Passwords for Admin Users should contain both numeric and alphabetic characters.	Failed	Enforce and configure the Password Policy in the Admin Security Settings to require at least one Letter and one Digit.	8.2.3
Minimum password length for Web Users is at least 7 characters.	Failed	Configure the Password Policy in the Web User Settings to require a 'Minimum Password Length' of 7 or more characters.	8.2.3
Passwords for Web Users should contain both numeric and alphabetic characters.	Failed	Configure the Password Policy in the Web User Settings to require at least one Letter and one Digit.	8.2.3
For Web Users that authenticate against the GoAnywhere login method, the maximum password age is 90 days or less.	Passed		8.2.4
For Web Users that authenticate against the GoAnywhere login method, the password expiration interval is 90 days or less.	Failed	The following Web Users should be configured to have a 'Password Expiration Interval' of 90 days or less: fosterj LinomaTest jfosterdev AMiller testimport ... and 9 other web users	8.2.4
For Admin Users that authenticate against the GoAnywhere login method, the maximum password age is 90 days or less.	Failed	Enable and configure the Password Policy in the Admin Security Settings to require the Maximum Password Age of 90 days or less.	8.2.4
For Web Users that authenticate against the GoAnywhere login method, they are not allowed to reuse their last 4 passwords.	Failed	Configure the Password Policy in the Web User Settings to enforce password history and disallow the reuse of the last 4 passwords.	8.2.5

Security Check	Status	Recommendation	PCI DSS Section
Admin Users that authenticate against the GoAnywhere login method are not allowed to reuse their last 4 passwords.	Failed	Enable and configure the Password Policy in the Admin Security Settings to enforce password history and disallow the reuse of the last 4 passwords.	8.2.5
For Web Users that authenticate against the GoAnywhere login method, their password must be changed after the first login.	Failed	The following Web User Templates should be configured to force password change at next login: 'Business Partners' 'Internal' 'no Address Book permissions' 'Product1Template_External' 'NortonUseCase'	8.2.6
All Admin Users are utilizing multi-factor authentication.	Failed	The 'root' and/or 'administrator' users are currently enabled. These are default accounts that only use the internal GoAnywhere login method and cannot be configured for multi-factor authentication.	8.3.1
All Web Users are utilizing multi-factor authentication for 'HTTPS'.	Failed	SAML is enabled, however it is not configured to force IDP authentication. The following Web Users should be configured to use multi-factor authentication for 'HTTPS': JFoster jfosterexample john.doe testingTemplate jfostertest	8.3.2
All Web Users are utilizing multi-factor authentication for 'AS2'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'AS2': JFoster testingTemplate jfostertest	8.3.2
All Web Users are utilizing multi-factor authentication for 'AS4'.	Passed		8.3.2
All Web Users are utilizing multi-factor authentication for 'FTPES'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'FTPES': JFoster testingTemplate jfostertest	8.3.2
All Web Users are utilizing multi-factor authentication for 'FTPS'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'FTPS': JFoster testingTemplate jfostertest	8.3.2
All Web Users are utilizing multi-factor authentication for 'SFTP'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'SFTP': JFoster jfosterexample john.doe testingTemplate jfostertest	8.3.2
All Web Users are utilizing multi-factor authentication for 'GoFast'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'GoFast': JFoster testingTemplate jfostertest	8.3.2
Anonymous users are not allowed to access services.	Failed	Configure the Web User Settings to disable the Anonymous Web User.	8.5

Security Check	Status	Recommendation	PCI DSS Section
At least 3 months of Audit Trails are immediately available for analysis.	Failed	Within the Log Settings, configure the following Audit Logs to not purge within 90 days: 'HTTPS Audit Logs'	10.7
Audit Trails are archived to disk if they are purged within 1 year.	Passed		10.7