10ZiG Security Vulnerability Testing Policy

As part of the normal 10ZiG firmware release cycle, firmware versions are scanned using the OpenVAS by Greenbone Security tool (http://www.openvas.org). These reports are included in the overall test results sent to R/D. As a policy, firmware with critical vulnerabilities CANNOT be released.

Because these types of vulnerabilities are constantly changing, we have included a list below of those identified by 10ZiG as well as the firmware versions in which they were resolved. If there is a vulnerability which has not been addressed, please send scan results to security@10zig.com with a relevant email address.

Regards,

10ZiG Technical Support

10ZiG Secure Thin & Zero Clients				
Vulnerability	**Date**	**Vulnerability Description**	**Suggested Solution**	**10ZiG Response**
VNC remote control service installed with no authentication (backdoor-vnc-0002)	7/24/2018	AT&T Virtual Network Computing (VNC) provides remote users with access to the system it is installed on. This installation appears to be using no authentication mechanism.	Remove or disable this service.	In the client VNC control panel make sure the VNC mode is set to either "Disabled" or "On Demand". This will close the VNC port.
VNC remote control service installed (backdoor-vnc-0001)	7/24/2018	AT&T Virtual Network Computing (VNC) provides remote users with access to the system it is installed on.	Remove or disable this service.	In the client VNC control panel make sure the VNC mode is set to "Disabled" or "On Demand". This will close the VNC port.

Vulnerability	Date	Vulnerability Description	Suggested Solution	10ZiG Response
X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	7/24/2018	The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.	Generate a new certificate usually signed by a trusted Certification Authority (CA)	10ZiG uses the certificate to encrypt communications with the management software. It is not used to identify the system.
Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)	7/24/2018	The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted.	Generate a new certificate usually signed by a Certification Authority (CA)	10ZiG uses the certificate to encrypt communications with the management software. It is not used to identify the system.
TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast)	7/24/2018	Weak ciphers for TLS 1.0/1.1	The only option is to disable the affected protocols (SSLv3 and TLS 1.0).	Fixed in NOS >= 10.12.157; PKOS >= 12.0.128.5
Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	7/24/2018	Self-signed certificates cannot be trusted by default	Generate a new certificate usually signed by a trusted Certification Authority (CA)	10ZiG uses the certificate to encrypt communications with the management software. It is not used to identify the system.
TLS Server Supports TLS version 1.0 (tlsv1_0-enabled)	7/24/2018	The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2	Disable TLS 1.0/1.1	Fixed in NOS >= 10.12.157; PKOS >= 12.0.128.5
Unencrypted X11 Service Available (x11-open-port)	7/24/2018	XWindows is an unencrypted protocol, as such it sends sensitive data in clear text.	Stop the X Server from listening on TCP ports, ensure it is running with: -nolisten tcp	Fixed in NOS >= 10.12.157.6; PKOS >= 12.0.129
TLS/SSL Server Supports The Use of Static Key Ciphers (ssl-static-key-ciphers)	7/24/2018	The server is configured to support ciphers known as static key ciphers.	Configure the server to disable support for static key cipher suites.	Turn off the SSL server in the Security Settings of the thin client

10ZiG Technology | US P: +1 (866) 865-5250 E: info@10ZiG.com | EMEA P: +44 (0) 116 214 8650 E: info@10ZiG.eu

Vulnerability	Date	Vulnerability Description	Suggested Solution	10ZiG Response
TLS/SSL Server Is Using Commonly Used Prime Numbers (tls-dh-primes)	7/24/2018	The server is using a common or default prime number as a parameter during the Diffie-Hellman key exchange.	Configure the server to use a randomly generated Diffie-Hellman group.	Turn off the SSL server in the Security Settings of the thin client
SHA-1-based Signature in TLS/SSL Server X.509 Certificate (tls-server-cert-sig-alg-sha1)	7/24/2018	The SHA-1 hashing algorithm has known weaknesses that expose it to collision attacks	Stop using signature algorithms relying on SHA-1, such as "SHA1withRSA".	Turn off the SSL server in the Security Settings of the thin client
TLS Server Supports TLS version 1.1 (tlsv1_1-enabled)	7/24/2018	The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2	Disable TLS 1.0/1.1	Fixed in NOS >= 10.12.157; PKOS >= 12.0.128.5
Nonexistent Page (404) Physical Path Disclosure 443	7/24/2018	Server notification of page which doesn't exist	Upgrade the web server to the latest version. Alternatively, reconfigure the web server to disable debug reporting.	
SMB Signing Disabled 445	7/24/2018	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	Remove samba package from build	NOS - N/A, Fixed in PKOS >= 12.0.129
Empty password field in /etc/passwd:User usbmux [user]	7/24/2018	Secure the account with a strong password in case the account is still in use, provide a strong password. If it is not in use currently either delete the account or deactivate it by locking it and setting the login shell to /dev/null. Use the following command to deactivate it:	Use secure passwords	These accounts are for internal use only. And cannot be used to access the system.
Click Jacking 443	7/24/2018	"Use HTTP X-Frame-Options Send the HTTP response headers with X-Frame-Options that instruct the browser to restrict framing where it is not allowed."	Limit access to web server	The thin client web server is used only by the management software. Cannot browse the contents…