10ZiG Security Vulnerability Testing Policy

As part of the normal 10ZiG firmware release cycle, general availability (GA) 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 10ZiG Research and Development department. 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.

Please note that whilst 10ZiG take every effort possible to ensure that this information is updated and correct, 10ZiG accept no responsibility or liability for errors, omissions or other inaccuracies. 10ZiG encourage their customers to actively perform their own security vulnerability testing, using 3rd party tools suitable to their own requirements and in order to be verified against any security compliance policy that may exist.

Each successive 10ZiG firmware and 10ZiG Manager release will include any resolved vulnerabilities in the release notes for that particular version. Please ensure that when seeking resolution for a specific vulnerability that the release notes for successive versions are checked as the particular issue may have been resolved in a later version.

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.

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
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.

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
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…
CVE-2000- 0869 CWE-693	3/5/2019	The installation of LightHTTPd enables WebDAV, which allows remote attackers to list arbitrary diretories via the PROPFIND HTTP request method.	Limit access to web server	We use WebDAV for client management. The only directory that is truly viewable is /upload. We store new packages in this directory during the update process. This is a temporary directory that is created on a system reboot so any files in the directory will be lost during the reboot process. While it is possible for multiple people to view webpages provided by the client, no pages provided by the server permit any user interaction. As such, it is not possible to execute a click-jacking attack against the webserver.
CVE-2017-9078	12/1/2019	The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.	Upgrade dropbear SSH server	Upgrade dropbear SSH server to v2018.76
CVE-2017-9079	12/1/2019	Dropbear before 2017.75 might allow local users to read certain files as root, if the file has the authorized_keys file format with a command= option. This occurs because ~/.ssh/authorized_keys is read with root privileges and symlinks are followed.	Upgrade dropbear SSH server	Upgrade dropbear SSH server to v2018.76

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
SSH server ciphers	11/30/2019	Dropbear SSH server not compatible with latest SSH cipher suites	Upgrade dropbear SSH server	Upgrade dropbear SSH server to v2018.76
CVE-2018-15599	10/18/2019	The recv_msg_userauth_request function in svr-auth.c in Dropbear through 2018.76 is prone to a user enumeration vulnerability because username validity affects how fields in SSH_MSG_USERAUTH messages are handled, a similar issue to CVE-2018-15473 in an unrelated codebase.	Upgrade dropbear SSH server	Upgrade dropbear SSH server to v2018.76
CVE 2018-19052	1/13/2020	An issue was discovered in mod_alias_physical_handler in mod_alias.c in lighttpd before 1.4.50. There is potential ../ path traversal of a single directory above an alias target, with a specific mod_alias configuration where the matched alias lacks a trailing '/' character, but the alias target filesystem path does have a trailing '/' character.	Upgrade lighttpd web server	Upgrade lighttpd web server to 1.4.54
Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.	1/15/2020	Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server. - Enabled DELETE method: This might allow an attacker to delete additional files on this web server.	Limit access to web server	We use WebDAV for client management. We store new packages in this directory during the update process. The /upload directory is a temporary directory that is used by our management software during the upgrade process. It is created/recreated during a system reboot so any files in the directory will be lost during the reboot process. While it is possible to Put/Delete files on the webserver, the /upload directory is not browsable so it is not possible to execute any malicious code/scripts that might be placed in the directory.

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
CVE-2021-44228	12/13/2021	Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.	10ZiG current releases, to include the 10ZiG Manager, NOS-64, PKOS-64, PKOS (32-bit), RePurpOS, and 10ZiG's stock Windows 10 builds do not contain Log4j.	On completion of the investigation 10ZiG confirm that the products and tested versions do not contain presence of Log4j and are not at risk of this security vulnerability. However due to the wide array of firmware and software versions in deployment, customers are advised to satisfy their own security requirements and perform security audits, focusing first on internet- facing devices and services.
Multiple CVE – InsydeH20 UEFI Software impacted by multiple vulnerabilities in SMM	3/21/2022	Multiple vulnerabilities have been found in Insyde UEFI BIOS. These affect the Insyde H2O UEFI firmware used on some 10ZiG clients. At present this effects the 6000q and 6100 series.	Set a UEFI password Do not allow booting from USB storage media	Contact 10ZiG Technical Support for access to updated BIOS or details as per suggested solution.
Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.	10/27/2022	Lighttpd daemon allows for PUT and DELETE methods in firmware.	Use “Block Port 80” check box in Security Settings applet of firmware and connect using the Cloud Connector method.	Disabling port 80 on the firmware mitigates this issue due to the web server no longer listening or responding on that port.

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

10ZiG Firmware Certificate Policy

10ZiG firmware contains CA certificates which can expire over time or become end of life. When this happens, it can cause a customer's VDI environment to become unusable until the expired certificates are upgraded or replaced. Obviously, this is a condition our customers would like to avoid. This statement addresses the issue of certificate expiration and how it can be mitigated.

1. The 10ZiG CA Certificate store is derived from the equivalent Ubuntu certificate store. As a company, 10ZiG will check the latest Ubuntu certificate store and automatically update the certificates for every firmware release as part of our release cycle. In addition, we will provide a firmware certificate add-on for every major firmware release (approximately every 3 months or once a quarter).
2. As a customer, if you have been notified by your vendor concerning a CA expiring, you can upgrade the certificate via the 10ZiG Management Utility (or a USB drive). These instructions are available in a separate guide.
3. All 10ZIG thin clients (Windows and Linux) support the Simple Certificate Enrollment Protocol (SCEP). This allows a customer to set up a certificate store on a network server from which the CA store on the thin clients can be upgrade automatically.

Sincerely,

10ZiG Technical Support

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