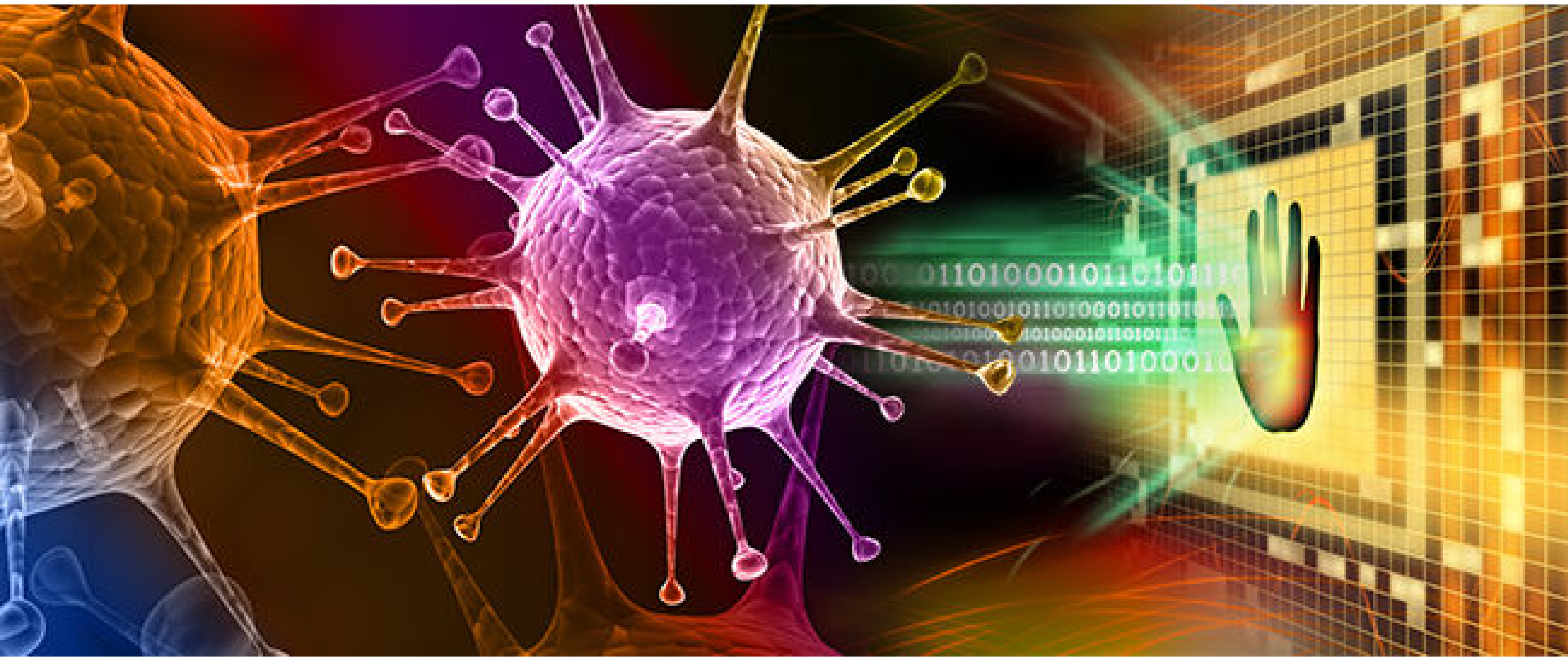


Security Component Audit Report

Secomea

January 26th 2024

TG alpha GmbH

Ulrichsberger Str. 17
94469 Deggendorf
Germany

Phone:	+49.991.402.271-00
Fax:	+49.991.402.271-99
Email:	info@tgalpha.de
Web:	https://www.tgalpha.de

Contents

© 2023 by TG alpha GmbH. All rights reserved.

Executive Summary

TG alpha GmbH was contracted by Secomea to conduct a security audit of the following components for industrial control systems. Since there was a full audit conducted on the last major release, which has only small differences to this latest minor release, this audit can be considered a smaller retest of the components. The product security audit was carried out with the following goals:

- Identification of potential new vulnerabilities within the implementation in regards to the changes
- Determination of the potential risk based on the newly discovered vulnerabilities

All tests and actions were conducted under controlled conditions. Also the web front end for the hardware components as well as the software implementations have been tested for known vulnerabilities and flaws in regard to the OWASP Top 10 list. A targeted penetration test with state of the art penetration testing tools has been conducted in order to evaluate the potential risk of potential vulnerabilities in the implementation of the components.

Important
As stated above, this audit can be considered an extension of the preceding audits from July 2023 and December 2023. Because of this, only results which differ from the last results will be documented. Furthermore no fuzzing tests have been conducted. The tests focus on covering changes from the prior version. Below the results is a changelog covering the changed findings from the last tests.

Tested Components

- GateManager with version 11.1.624032003
- GateManager API
- SiteManager with version 11.1.624032003
- SiteManager Embedded with version 11.0.624032003
- LinkManager with version 11.1.624032003

Out-Of-Scope Components

- Data Collection Module (DCM)

© 2023 by TG alpha GmbH. All rights reserved.

Results:
The audit was successfully passed. The hardware and software components were tested for vulnerabilities. Therefore a vulnerability assessment, exploitation and analysis of communication principles were done. The result of the component audit is that all components are robust against the most common attacks.

Changelog - Regression test from January 26th 2024

GateManager

- A new vulnerability for the used jQuery-Mobile v.1.3.2 has been found: 1.4

SiteManager

- No new findings

SiteManager Embedded

- No new findings

LinkManager

- No new findings

© 2023 by TG alpha GmbH. All rights reserved.

Discovered New Vulnerabilities with Criticality				
Component	high	medium	low	informational
GateManager - Admin	0(0)	0(0)	0(0)	0(0)
GateManager - LinkManager	0(0)	0(0)	0(0)	0(0)
GateManager - LinkManager Mobile	0(0)	0(0)	0(0)	0(0)
SiteManager	0(0)	0(0)	0(0)	0(0)
SiteManager Embedded	0(0)	0(0)	0(0)	0(0)
LinkManager	0(0)	0(0)	0(0)	0(0)
Numbers in brackets includes vulnerabilities which are marked as *not relevant*, *resolved* or *false positives*				

Suggestions

According to the audit results following suggestions are proposed:

- See last report’s recommendations

No new recommendations have been issued.

© 2023 by TG alpha GmbH. All rights reserved.

1 Component Audit

1.1 Test Environment

Secomea provided Updates to the GateManager and the SiteManager firmware. As such the system under consideration (SuC) consists mainly of the GateManager and the SiteManager and implicitly LinkManager Mobile. The results for the LinkManager Mobile have been compilated into the GateManager results. Secomea provided the documentation of the SuC to TG alpha. In the audit all ethernet interfaces were considered. It is assumed that Secomea truthfully answered questions and the implementation and documentation of all functions is as described in the documentation.

Lab Setup for the Audit

By default, all hardware firewalls in the network are configured that connections from inside to outside will be permitted and all connections from outside to inside are blocked. Therefore no additional configuration is required for commissioning of the Secomea GateManager and GateManager API.

The test systems were the following:

- GateManager with version 11.1.624032003 on an installed/updated Ubuntu 22.04.2
- SiteManager with version 11.1.624032003
- SiteManager Embedded with version 11.0.624032003 on an installed/updated Ubuntu 22.04.2
- LinkManager with version 11.1.624032003 on an installed/updated Windows 10 Pro

Due to the declarations (see appendix) of the similarities of the different SiteManager generations and variations, the SM3549 is considered the representative device for the audit.

© 2023 by TG alpha GmbH. All rights reserved.

1.2 Verification of Attack Surface

CVE Findings

This table lists all found CPEs of the used third party software listed with the according numbers of CVEs. The Common Platform Enumeration is the list of all listed programs/libraries, etc. in the Nation Vulnerability Database (NVD) of NIST[1]. The most import parts of a CPE are vendor, product and version number. The Common Vulnerabilites and Exposures (CVE) are linked to CPEs. Some used technologies don't have CPEs. To find their corresponding CVEs a npm search has been conducted on the snyk Vulnerability Database[2]. They can be distinguished from normal CPEs by the @-sign between product and version number.

This table was created in June when the first tests were done and has been updated for this minor version.

GateManager

CPE List with CVE count				
CPE	Critical	High	Medium	Low
jquery-mobile@1.3.2	0	0	1	0
jquery-ui@1.13.3-pre	0	0	0	0
jquery@3.6.0	0	0	0	0
jquery-migrate@3.3.2	0	0	0	0
jquery-ui-timepicker-addon@1.6.3	0	0	0	0

SiteManager

CPE List with CVE count				
CPE	Critical	High	Medium	Low
denx:u-boot:2018.07	18	7	2	0
w1.fi:hostapd:2.9	2	0	2	0
arm:mbed_tls:2.28.5	0	2	1	0
openssl:openssl:1.1.1w	0	1	2	0
open62541:open62541:1.1.2	0	1	0	0
xmlsoft:libxml2:2.11.5	0	0	1	0
json-c:json-c:0.17-20230812	0	0	0	0
sqlite:sqlite:3.44.2	0	0	0	0

[1] https://nvd.nist.gov

[2] https://security.snyk.io/

© 2023 by TG alpha GmbH. All rights reserved.

tuxfamily:chrony:3.5.1	0	0	0	0
kernel:iw:5.9	0	0	0	0
libcap-ng_project:libcap-ng:0.7.9	0	0	0	0
netfilter:libmnl:1.0.4	0	0	0	0
libmodbus:libmodbus:3.1.8	0	0	0	0
libnl_project:libnl:3.5.0	0	0	0	0
tcpdump:libpcap:1.9.1	0	0	0	0
snap7_project:snap7_server:1.4.2	0	0	0	0
rng-tools_project:rng-tools:5.0	0	0	0	0
jquery-ui@1.13.3-pre	0	0	0	0
jquery@3.6.0	0	0	0	0
jquery-migrate@3.3.2	0	0	0	0
jquery-ui-timepicker-addon@1.6.3	0	0	0	0

For the Linux Kernel v. 5.15.127+ 0 CVEs have been found.

Secomea Comment
A CI pipeline is in place to inform the customer of any CVEs which might affect their systems. The customer deals with these discoveries accordingly.

1.3 Port Analysis

This section contains the information scanning the ports and connecting with netcat. For determining the standard usage of the ports the reference by the Internet Assigned Numbers Authority (IANA)[3] is considered.

Port scanning is done with nmap with the port range 1-65535. Additionally if possible the OS was used to identify any other open network ports.

GateManager

Port Scan

Port	IANA Definition	Comment
TCP		
5	Remote Job Entry	CRM Web API, implementable service, port choosable in server config, secured via Access Control
22	SSH	implementable service, port choosable in server config
23	Telnet	implementable service, port choosable in server config
80	HTTP	redirect to HTTPS
443	HTTPS	
777	Multiling HTTP	Debug Console (Telnet), implementable service, port choosable in server config
778	Unassigned	Management Console localhost only
3389	ms-wbt-server	RDP, implementable service, port choosable in server config
4822	Unassigned	GUACD docker localhost only
5800	vnc-http	VNC, implementable service, port choosable in server config
5900	vnc	Java VNC, implementable service, port choosable in server config
11444	Unassigned	GoToAppliance port, port choosable in server config

Remaining Ports
The remaining TCP Ports are closed.

[3] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

All UDP Ports are filtered, thus not allowing any communication.

1.3.1 SiteManager

Port Scan - DEV Interface

Port	IANA Definition	Comment
TCP		
23	Telnet	Implementable service, port choosable in server config
53	Domain Name Server	
443	HTTPS	
8080	HTTP-proxy	Web Proxy Relay port, implementable service, port choosable in server config
UDP		
53	Domain Name Server	
68	DHCP	filtered

Port Scan - UPLINK Interface

Port	IANA Definition	Comment
TCP		
23	Telnet	Implementable service, port choosable in server config
443	HTTPS	
UDP		
68	DHCP	filtered

1.3.2 SiteManager Embedded

Port Scan

Port	IANA Definition	Comment
TCP		
11444	Unassigned	SiteManager Embedded web app Bound to localhost

The SiteManager Embedded does not have any ports open to the network.

1.3.3 LinkManager

Port Scan

Port	IANA Definition	Comment
TCP		
11445	Unassigned	LinkManager Mobile web app Bound to LinkManagerTray.exe Bound to localhost

The LinkManager does not have any ports open to the network.

© 2023 by TG alpha GmbH. All rights reserved.

1.4 Web Technology Analysis

This section contains the information scanning the web applications in terms of used technologies. This is done using the browser plugin Wappalyzer. This section is supplemented with the results of the plugin retire.js which detects obsolete or vulnerable versions.

GateManager

Technology	Detected Version	Comment
HSTS		
jQuery	3.6.0	
jQuery Migrate	3.3.2	
jQuery Mobile	1.3.2	Vulnerable version
jQuery UI	1.13.0	Manual review revealed that version 11.1.624032003 is used, which is a WIP build of jQuery UI (v1.13.3-pre).

Found CVEs

Technology	Name / CVEs of vulnerability
jQuery Mobile	Medium XSS vulnerability

SiteManager

Technology	Detected Version	Comment
Apache Web Server		
HSTS		

1.5 Greenbone Vulnerability Manager

With the Greenbone Vulnerability Manager (GVM v. 21.4.4, previously OpenVAS) the components have been checked for known vulnerabilities. The following tables report the findings of the performed Network Vulnerability Scans (NVTs) with respect to the Common Vulnerabilities and Exposures[4] (CVE) database as well as the corresponding Common Vulnerability Scoring System (CVSS) value stemming from a standardized method for rating IT vulnerabilities. Any component that is not reachable via network was not considered.

All GVM scans were performed with following Feed Versions:

- NVT Feed Version 20230612T0554
- SCAP Feed Version 20230612T0913
- CERT Feed Version 20230612T0406
- GVMD DATA Feed Version 20230612T0503

1.5.1 GateManager

No new vulnerabilities have been discovered.

1.5.2 SiteManager

No new vulnerabilities have been discovered.

Conclusion

No relevant issues exist.

[4] `https://cve.mitre.org/`

1.6 OWASP ZAP

For the audit the OWASP ZAP 2.14.0 test has been configured to allow for more false positives. To verify that issues exist the warnings have been tested with the Firefox Developer Tools, etc.

1.6.1 GateManager | Port 443

No new vulnerabilities have been discovered.

1.6.2 SiteManager | Port 443

No new vulnerabilities have been discovered.

1.6.3 SiteManager - Embedded | Port 11444

No new vulnerabilities have been discovered.

1.6.4 LinkManager | Port 11445

No new vulnerabilities have been discovered.

1.6.5 Conclusion

No critical issues exist. As stated in the last reports anti-CSRF tokens as well as CSP should be added.

© 2023 by TG alpha GmbH. All rights reserved.

1.7 SSL Testing

To verify the connection encryption of the GateManager the tool testssl.sh[5] version 3.0.8 has been used. It checks for which protocols and ciphers are implemented and if it can detect vulnerabilites.

Also SSLyze is used to augment the test results.

1.7.1 GateManager

Protocol	**Status**
SSLv2	not offered**(OK)**
SSLv3	not offered**(OK)**
TLS 1.0	not offered**(OK)**
TLS 1.1	not offered**(OK)**
TLS 1.2	offered**(OK)**
TLS 1.3	not offered and downgraded to a weaker protocol
NPN/SPDY	not offered
ALPN/HTTP2	not offered

Standard cipher categories	**Status**
NULL ciphers (no encryption)	not offered**(OK)**
Anonymous NULL Ciphers (no authentication)	not offered**(OK)**
Export ciphers (w/o ADH+NULL)	not offered**(OK)**
LOW: 64 Bit + DES, RC[2,4] (w/o export)	not offered**(OK)**
Triple DES Ciphers / IDEA	not offered
Obsoleted CBC ciphers (AES, ARIA etc.)	not offered
Strong encryption (AEAD ciphers)	not offered
Forward Secrecy (FS)	offered**(OK)**
Elliptic curves offered:	prime256v1 secp384r1 secp521r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1 X25519 X448
Has server cipher order?	yes**(OK)**
X-XSS-Protection	1 mode=block**(OK)**

. . . continues on next page . . .

[5] `https://testssl.sh/`

© 2023 by TG alpha GmbH. All rights reserved.

. . . continued from previous page . . .

X-Content-Type-Options	nosniff**(OK)**
Content-Security-Policy	default-src 'self'; img-src 'self' data:; frame-src 'self'; form-action 'self'; base-uri 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'

Protocol	**Cipher**
TLSv1.2:	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Possible Vulnerabilities	**Status**
Heartbleed (CVE-2014-0160)	not vulnerable **(OK)**, no heartbeat extension
CCS (CVE-2014-0224)	not vulnerable **(OK)**
Ticketbleed (CVE-2016-9244), experiment.	not vulnerable **(OK)**
ROBOT	Server does not support any cipher suites that use RSA key transport
Secure Renegotiation (RFC 5746)	supported **(OK)**
Secure Client-Initiated Renegotiation	not vulnerable **(OK)**
CRIME, TLS (CVE-2012-4929)	not vulnerable **(OK)**
BREACH (CVE-2013-3587)	no HTTP compression **(OK)** - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)	not vulnerable **(OK)**, no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)	No fallback possible **(OK)**, no protocol below TLS 1.2 offered
SWEET32 (CVE-2016-2183, CVE-2016-6329)	not vulnerable **(OK)**
FREAK (CVE-2015-0204)	not vulnerable **(OK)**
DROWN (CVE-2016-0800, CVE-2016-0703)	not vulnerable on this host and port **(OK)** make sure you don't use this certificate elsewhere with SSLv2 enabled services
LOGJAM (CVE-2015-4000), experimental	not vulnerable **(OK)**: no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
BEAST (CVE-2011-3389)	not vulnerable **(OK)**, no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental	not vulnerable **(OK)**
Winshock (CVE-2014-6321), experimental	not vulnerable **(OK)** - CAMELLIA or ECDHE_RSA GCM ciphers found

. . . continues on next page . . .

© 2023 by TG alpha GmbH. All rights reserved.

. . . continued from previous page . . .

RC4 (CVE-2013-2566, CVE-2015-2808)	no RC4 ciphers detected **(OK)**

Additional SSLyze Results	**Status**
Deflate Compression	Compression disabled **(OK)**
TLSv1.2 Forward Secrecy	offered **(OK)**
Legacy RC4 Algorithm	not offered **(OK)**
Client Renegotiation DoS Attack	not vulnerable **(OK)**
Secure Renegotiation	supported **(OK)**

Conclusion

The GateManager uses a well configured TLS encryption (TCP port 443).

1.7.2 SiteManager

Protocol	**Status**
SSLv2	not offered**(OK)**
SSLv3	not offered**(OK)**
TLS 1.0	not offered**(OK)**
TLS 1.1	not offered**(OK)**
TLS 1.2	offered**(OK)**
TLS 1.3	offered**(OK)**: final
NPN/SPDY	not offered
ALPN/HTTP2	not offered

Standard cipher categories	**Status**
NULL ciphers (no encryption)	not offered**(OK)**
Anonymous NULL Ciphers (no authentication)	not offered**(OK)**
Export ciphers (w/o ADH+NULL)	not offered**(OK)**
LOW: 64 Bit + DES, RC[2,4] (w/o export)	not offered**(OK)**
Triple DES Ciphers / IDEA	not offered
Obsoleted CBC ciphers (AES, ARIA etc.)	not offered
Strong encryption (AEAD ciphers)	offered**(OK)**
Forward Secrecy (FS)	offered**(OK)**
Elliptic curves offered:	prime256v1 secp384r1 secp521r1 X25519 X448
Has server cipher order?	yes**(OK)** – TLS 1.3 and below

. . . continues on next page . . .

. . . continued from previous page . . .

X-XSS-Protection	1 mode=block**(OK)**
X-Content-Type-Options	nosniff**(OK)**
Content-Security-Policy	default-src ’self’; script-src ’self’ ’nonce-MCHNTNt0OrgXzAAQD0j0CA==’; style-src ’self’ ’nonce-MCHNTNt0OrgXzAAQD0j0CA==’; form-action ’self’; frame-ancestors ’self’; base-uri ’none’

Protocol	**Cipher**
TLSv1.2:	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_256_CCM_8 TLS_RSA_WITH_AES_256_CCM TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_128_CCM_8 TLS_RSA_WITH_AES_128_CCM
TLSv1.3:	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256

Possible Vulnerabilities	**Status**
Heartbleed (CVE-2014-0160)	not vulnerable **(OK)**, no heartbeat extension
CCS (CVE-2014-0224)	not vulnerable **(OK)**
Ticketbleed (CVE-2016-9244), experiment.	not vulnerable **(OK)**
ROBOT	not vulnerable **(OK)**
Secure Renegotiation (RFC 5746)	supported **(OK)**
Secure Client-Initiated Renegotiation	not vulnerable **(OK)**
CRIME, TLS (CVE-2012-4929)	not vulnerable **(OK)**
BREACH (CVE-2013-3587)	no HTTP compression **(OK)** - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)	not vulnerable **(OK)**, no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)	No fallback possible **(OK)**, no protocol below TLS 1.2 offered

. . . continues on next page . . .

. . . continued from previous page . . .

SWEET32 (CVE-2016-2183, CVE-2016-6329)	not vulnerable **(OK)**
FREAK (CVE-2015-0204)	not vulnerable **(OK)**
DROWN (CVE-2016-0800, CVE-2016-0703)	not vulnerable on this host and port **(OK)** make sure you don't use this certificate elsewhere with SSLv2 enabled services
LOGJAM (CVE-2015-4000), experimental	not vulnerable **(OK)**: no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
BEAST (CVE-2011-3389)	not vulnerable **(OK)**, no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental	not vulnerable **(OK)**
Winshock (CVE-2014-6321), experimental	not vulnerable **(OK)**
RC4 (CVE-2013-2566, CVE-2015-2808)	no RC4 ciphers detected **(OK)**

Conclusion

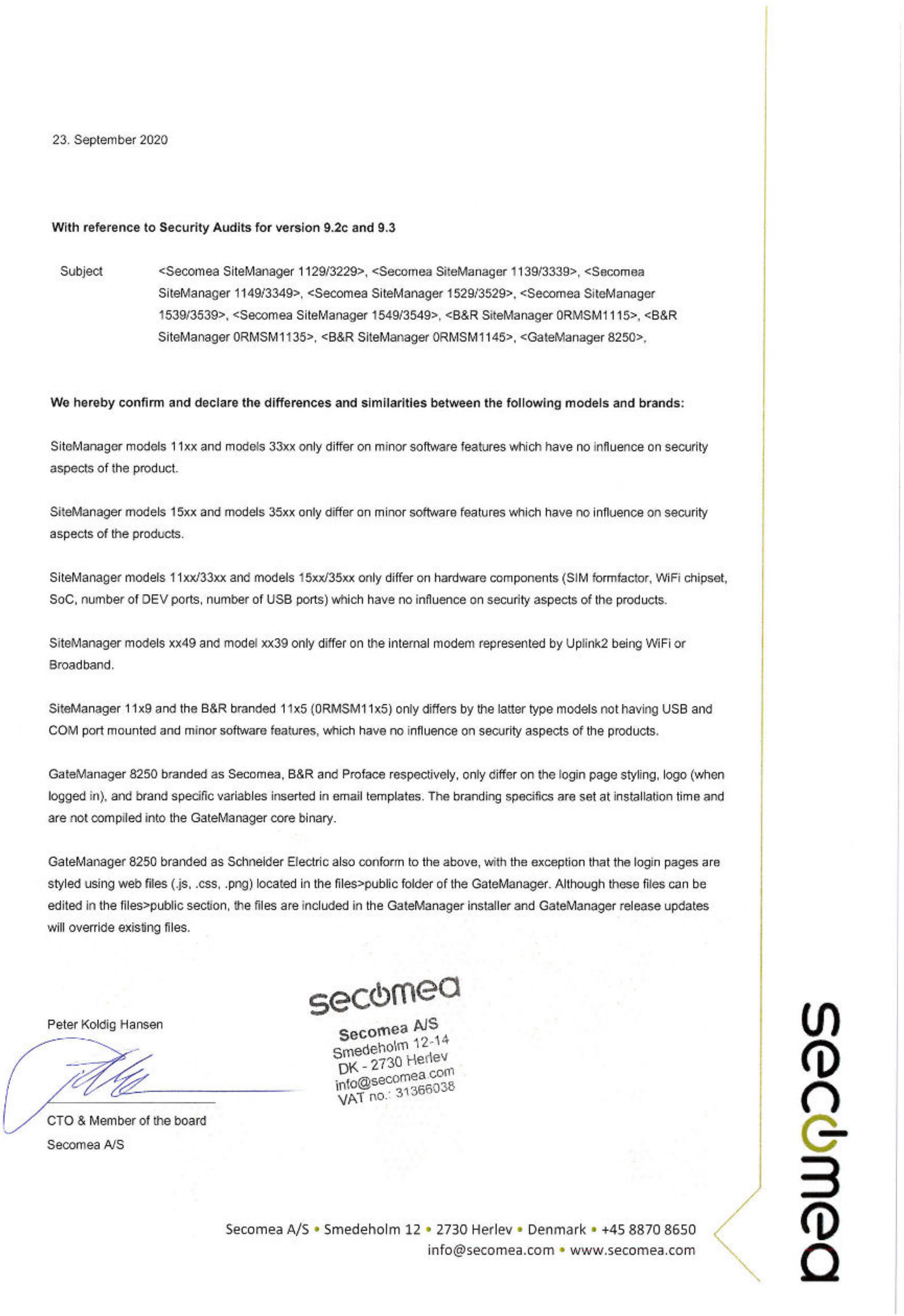
The SiteManager uses a well configured TLS encryption (TCP port 443).

2 Audit Conclusion

All components were tested for vulnerabilities. No critical vulnerability exists. All latest components are robust against the most common attacks.

As a result of all tests the security audit has successfully passed.

© 2023 by TG alpha GmbH. All rights reserved.



23. September 2020

With reference to Security Audits for version 9.2c and 9.3

Subject <Secomea SiteManager 1129/3229>, <Secomea SiteManager 1139/3339>, <Secomea SiteManager 1149/3349>, <Secomea SiteManager 1529/3529>, <Secomea SiteManager 1539/3539>, <Secomea SiteManager 1549/3549>, <B&R SiteManager 0RMSM1115>, <B&R SiteManager 0RMSM1135>, <B&R SiteManager 0RMSM1145>, <GateManager 8250>,

We hereby confirm and declare the differences and similarities between the following models and brands:

SiteManager models 11xx and models 33xx only differ on minor software features which have no influence on security aspects of the product.

SiteManager models 15xx and models 35xx only differ on minor software features which have no influence on security aspects of the products.

SiteManager models 11xx/33xx and models 15xx/35xx only differ on hardware components (SIM formfactor, WiFi chipset, SoC, number of DEV ports, number of USB ports) which have no influence on security aspects of the products.

SiteManager models xx49 and model xx39 only differ on the internal modem represented by Uplink2 being WiFi or Broadband.

SiteManager 11x9 and the B&R branded 11x5 (0RMSM11x5) only differs by the latter type models not having USB and COM port mounted and minor software features, which have no influence on security aspects of the products.

GateManager 8250 branded as Secomea, B&R and Proface respectively, only differ on the login page styling, logo (when logged in), and brand specific variables inserted in email templates. The branding specifics are set at installation time and are not compiled into the GateManager core binary.

GateManager 8250 branded as Schneider Electric also conform to the above, with the exception that the login pages are styled using web files (.js, .css, .png) located in the files>public folder of the GateManager. Although these files can be edited in the files>public section, the files are included in the GateManager installer and GateManager release updates will override existing files.

Peter Koldig Hansen

CTO & Member of the board
Secomea A/S

secomea
Secomea A/S
Smedeholm 12-14
DK - 2730 Herlev
info@secomea.com
VAT no.: 31366038