pfSense Security Appliance

EVALUATION REPORT

for Rubicon Communications, LLC

CONFIDENTIAL / PROPRIETARY

Date:	18.10.2016
Updated:	20.12.2016
Version:	1.1
Author(s):	Paul Lam InfoSec Global 403-270 Albert Street, Ottawa Ontario, K1P 6N7, Canada Paul.Lam@infosecglobal.com 1 613 800 8964

NOTICE OF CONFIDENTIALITY

This document contains privileged and confidential information of InfoSec Global Inc. (“ISG”). Rubicon Communications LLC (Client) shall reproduce the document only as necessary to perform an evaluation, and will take all necessary and reasonable measures to prevent the unauthorized use, disclosure or distribution of the document or parts thereof.

Client shall not use, amend, translate, adapt, convert, or exploit the contents of this proposal without ISG’s written authorization nor allow ISG’s competitors to have access to its contents.

Revision History

Version	Date	Description	Authors
0.1	18/10/16	Initial Draft	Daniele Bastianello
0.2	27/10/16	Draft	Dan Bastianello, Paul Lam
0.3	28/10/16	Draft	Paul Lam
0.4	02/11/16	Draft	David Maxwell, Dan Bastianello
1.0	17/11/16	Final	David Maxwell, Dan Bastianello
1.1	13/12/16	Addendum	David Maxwell, Paul Lam

Table of Contents

Executive Summary **5**

References **6**

1 Introduction **7**

2 Acronyms and Definitions **7**

2.1 Acronyms 7

2.2 Definitions 7

3 Review Environment **8**

4 Assessment Scope **9**

5 Product Description **9**

5.1 Codebase Sizing 9

5.2 Language Characteristics 9

5.3 Third Party Components 10

6 Methodology **11**

6.1 SCA Methodology 11

6.2 VA Methodology 12

7 Findings **13**

7.1 Summary 13

7.2 General Findings 13

7.3 Detailed Findings 14

8 Conclusion **28**

Executive Summary

InfoSec Global was engaged by Rubicon Communications to perform a security-focused evaluation of the pfSense firewall distribution that is distributed on their Netgate network firewall appliances. Throughout the course of the assessment there were very few potential security concerns identified.

The configuration of the system users, file and process permissions implemented in the FreeBSD operating system is the underlying base that the pfSense appliance built upon providing a strong security foundation. Beyond that, the PHP server configuration along with a minimal use of externally exposed user input fields employed in the PHP orchestration layer further enhance it. Additionally, the use of the Suhosin patch and extension greatly improves security posture of any PHP application by going further than what configurations can by adding several advanced protection techniques such as protection against stack smashing techniques by using Canaries and SafeUnlink protection.

Recommendations and mitigation strategies were provided, however none of the findings observed in the white box analysis were deemed to be of a high or critical nature. Although the white box review did not yield any high or critical findings the third party components review did find some Common Vulnerability Enumerations (CVE) which have been deemed by the engagement team to be areas of concern and provided recommendations which should be reviewed.

References

This report used the following documents in its construction:

[1] NIST National Vulnerability Database[1]

[2] pfSense Documentation Site[2]

[3] CVSS 3.0 Calculator[3]

[4] Wikipedia (Package definitions)[4]

[1] https://nvd.nist.gov/
[2] https://doc.pfsense.org/index.php/Main_Page
[3] https://nvd.nist.gov/cvss/v3-calculator
[4] https://wikipedia.org

1 Introduction

Source code analysis is an important aspect of an overall security review program. Code review is the systematic examination of computer programming code intended to identify and correct weaknesses or flaws. Programming code can include code for software applications, firmware or hardware. Code review often takes place as part of the overall Software Development Lifecycle (SDLC) – and may include "peer review" among internal colleagues. In some cases, security sensitive organizations such as governments may require the source code of the product they are acquiring to be vetted by their own security personnel or by an independent third party.

InfoSec Global, is a third party organization which conducts source code review on behalf of security conscious clients or vendors. ISG was engaged by Rubicon Communications to conduct a Globus Cyber Assurance (GCA) IT security evaluation of a XG-2758-1U pfSense security appliance.

Figure 1. Netgate XG-2758-1U pfSense Security Appliance

This report details both the evaluation findings and the associated mitigation recommendations.

2 Acronyms and Definitions

2.1 Acronyms

GCA: Globus Cyber Assurance

ISG: InfoSec Global

ISO: International Standards Organization

IT: Information Technologies

QMS: Quality Management System

SCA: Source Code Analysis

SoS: Statement of Sensitivity

TOE: Target of Evaluation

2.2 Definitions

Client: Rubicon Communications LLC

3 Review Environment

The following table lists the ISG personnel who participated in the security evaluation of the Netgate XG-2758-1u security appliance:

Name	Title
Ahmed Techini	Technical Director
Paul Lam	Security Engineer
Daniele Bastianello	Security Engineer

Table 1. InfoSec Global engagement team

The client provided the appliance (Netgate XG-2758-1U) to the engagement team with default production configuration and the source code including the commercial features which are not included in the community edition. All evaluation activities were conducted in the ISG Globus Cyber Assurance facility based in Ottawa between early September to mid-October 2016.

4 Assessment Scope

The following components were considered in scope for the evaluation:

- **pfSense**: is the PHP driven orchestration layer graphical web interface developed and maintained by Rubicon Communications.
- **Amazon AWS plugin**: is a commercial plugin providing secure connectivity to the AWS services provided by Amazon.

For this evaluation, only the pfSense PHP orchestration layer and the Amazon AWS plugin were considered in scope. The third party components and the FreeBSD operating system as a whole were not considered in scope. Although the third party components and FreeBSD are not in scope; File/directory permissions, PHP directives/configurations and nginx configurations are considered in scope since they affect the security posture of the PHP implementation used to host the pfSense web interface and can change the behavior of a PHP application.

5 Product Description

This section details pertinent characteristics of the evaluated products.

5.1 Codebase Sizing

The following table details the line count and folder structure of the codebases evaluated by the engagement team:

Component	Language	Lines of Code (LoC)
pfSense	PHP	165,112
pfSense	JavaScript	16,919

Table 2. Codebase characteristics

5.2 Language Characteristics

Each programming language has specific characteristics which may factor into the focus of the assessment. The following subsection provides a high-level review of the PHP programming language as used in the assessed components.

5.2.1 PHP

PHP is a general purpose procedural language used primarily to provide server-side dynamic web service. Among its design goals are to allow for rapid prototyping, interaction with server-side databases and easy to manipulate HTML template responses.

Areas of concern within PHP are to ensure that various configuration items such as “magic_quotes_gpc” and “register_globals” are disabled; that error reporting is disabled in production; that SQL injection is mitigated through typical patterns; file inclusions are not web-accessible; and protection against all items within the OWASP top 10 Web vulnerabilities.

5.2.2 Javascript

Javascript is an interpreted scripting language frequently used for web applications on either the client or server side. In general scripting languages are often used as the glue to allow more flexibility to any web application with the added bonus of making it easier and faster to code than lower-level compiled languages such as C.

Areas of concern with Javascript are that it can provide potential malicious users a means to execute scripts on a client computer via the Web. The focus on these scripts will ensure mitigation techniques are employed regarding Cross-site Scripting; trust boundaries and OWASP top 10 Web vulnerabilities.

5.3 Third Party Components

Third party components are commonly included in source code packages to speed up development effort, leverage best of breed tools and mechanisms, and/or to provide interoperability to other functional pieces. Third party components are considered to be in-scope, though the level of focus can vary depending on assurance factors. The following subsections detail the relevant third party components/modules that are included in the pfSense Security appliance.

Component	Version	Description
FreeBSD	10.3 Release 5	FreeBSD is a free and open source Unix-like operating system descended from the Berkeley Software Distribution (BSD).
Ngnix	1.10.1	Ngnix is a free, open source, high-performance web server and reverse proxy, as well as an IMAP/POP3 proxy server.
BZip2	1.0.6	Bzip2 is a free and open-source file compression application which uses the Burrows-Wheeler algorithm.
PHP-FPM	5.6.23	PHP-FPM is a FastCGI Process Manager which is an alternative to the implementation of PHP's FastCGI.
cURL	7.49.1	cURL is a free and open-source program that provides a Client URL Request Library supporting several protocols.
OpenSSL	1.0.1s	OpenSSL is a general purpose cryptographic library that provides an open-source implementation of SSL and TLS protocols.
Zlib	1.2.8	zLib is a compression library.
LibXML	2.9.3	LibXML is a xml parsing library.
DOM/XML API	20031129	DOM (Data Object Model) defines a standard for accessing document formats such as XML and others.
JSON	1.2.1	JSON (JavaScript Object Notation) is a lightweight data-interchange format.
OpenLDAP	2.4.44	OpenLDAP is an open-source implementation of the Lightweight Directory Access Protocol.
Libmbfl	1.3.2	Libmbfl is depended upon by the mbstring set of functions. Mbstring is used to provide enhanced support for Simplified/Traditional Chinese, Korean, Japanese and Russian languages.
Libmcrypt	2.5.8	Libmcrypt is a library which provides a uniform interface to several symmetric encryption algorithms.

MYSQLND	5.0.11	This is the MySQL native driver for PHP which replaces the MySQL client library (libmysql).
PCRE	8.39	PCRE (Perl Compatible Regular Expressions) is a C library inspired by the regex capabilities in Perl.
SQLite	3.13.0	SQLite is a self-contained, serverless, zero-configuration transactional Structured Query Language database engine.
Radius	1.3.0	Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centeralized Authentication, Authorization, and Accounting management of network connected users.
Readline	5.2	Is a library that provides line editing and history capabilities to command line interfaces.
RRD Library	1.6.0	RRD is an open-source industry standard, high performance data logging and graphing system for time series data.
SSH2	1.17	Secure Socket Shell 2 is a more secure and efficient replacement for SSH which provides a network protocol that allows for a secure terminal connection to a remote host.
LibSSH2	1.7.0	Libraries used by the SSH service.
Suhosin	0.9.38	Suhosin is an advanced protection system for PHP installations. Desgined to protect users and servers from (un)known flaws in PHP core and applications.
xdebug	2.4.0	Xdebug is a PHP extension which provides debugging and profilling capabilities.
Libxml2	2.9.3	LibXML2 is a xml parsing library.
ZMQ extension	1.1.3	ZeroMQ is a library that decentralizes messaging and computing.
Libzmq	4.1.4	Libraries used by the ZeroMQ extension.
OpenVPN	2.3.11	OpenVPN is a open-source appliaction that implements a Virtual Private Network (VPN) tunnel for creating a secure point-to-point connection.
Zend Framework	2.6.0	Zend framework is a component library for PHP.
Simplepie	1.1.3	RSS parser written in PHP

6 Methodology

The assessment methodology employed by ISG for the Netgate security appliance security assessment can be divided into two sections: SCA methodology and VA methodology.

6.1 SCA Methodology

For this engagement, ISG employed both automated and manual code review approach to conduct the source code review. The analysis activities performed include but are not limited to:

- String searches:
  - Simple string searches
  - Magic constants (e.g. Base64-encoded values, hex-encoded values, etc.)
  - Developer comments (e.g. FIXME, TODO, HACK, CHECK, etc.)
  - Error control keywords (e.g. ERROR, FATAL, DIE, KILL, etc.)

    - Security-relevant keywords (e.g. user, uid, pwd, passwd, secret, root, etc.)
- Error-prone area searches:
    - Native code linkages
    - Use of file paths (may be prone to path traversal attacks)
    - Exception handling
- Logic analysis
- Non-standard API usage
- Tainted data tracing
- SCA tool scan and triage of findings

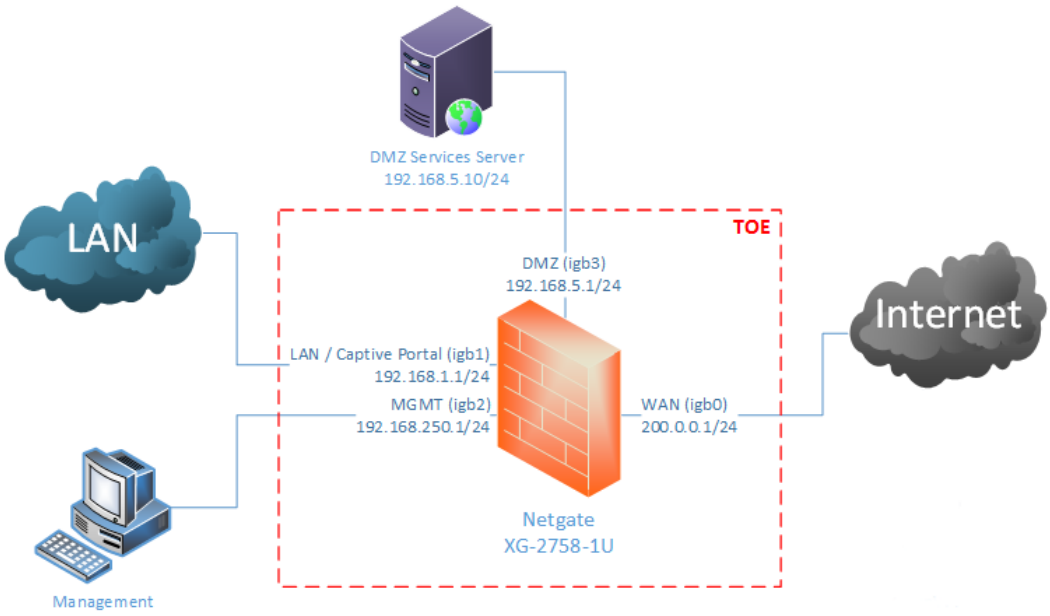
6.2 VA Methodology

For the VA portion of the security assessment, a Black Box[5] assessment methodology was employed. Software tools were used in combination with manual analysis and verification. Tool categories include:

- Network port scanners
- Web application scanners
- Network traffic analyzers
- Vulnerability scanners

All activities performed were conducted based on a scenario in which the TOE is the primary firewall appliance in an SMB environment. The engagement team focused on firewall traffic handling, verifying cryptographic implementations where applicable and the management UI.

The engagement team evaluation utilized the following network design layout:



[5] For Black Box assessments, the device, system or object is viewed in terms of its inputs and outputs, without any knowledge of its internal workings

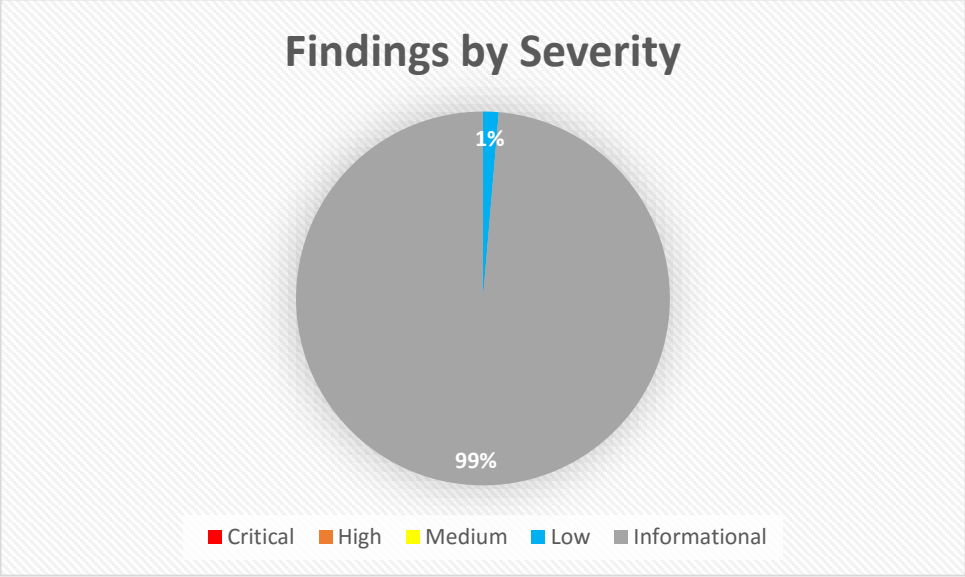
7 Findings

This section details the assessment findings. The engagement team adapted the Common Vulnerability Scoring System (CVSS) v3 standard to assign severity ratings to the findings. The CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The following table details the qualitative severity ratings scale used in the assessment:

Rating	CVSS Base Score
Informational	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

7.1 Summary

This section shows high-level metrics about the findings discovered during the secure assessment for the Netgate security appliance:



7.2 General Findings

This section contains general, high-level findings as determined by the engagement team over the course of the assessment.

7.2.1 pfSense 2.3.2

pfSense is an open source firewall/router appliance distribution based on FreeBSD. It utilizes several mechanisms provided by the operating system such as the employing a hardened service configuration and the inclusion of extensions and patches to help thwart many known weaknesses in

PHP. Throughout the course of this assessment the engagement team had reviewed several aspects of the Netgate appliance to evaluate its security posture. Having examined the OS configuration, it was apparent that several security conscious settings have been applied to help reduce the attack surface.

These sets of security related enhancements proved to be difficult to circumvent making pfSense a robust security conscious firewall distribution.

7.3 Detailed Findings

This section contains the detailed findings as determined by the engagement team over the course of the assessment.

7.3.1 pfSense 2.3.2

As the time of the report there were no outstanding CVEs associated with the deployed version of pfSense provided by the client. That said there are a few findings that should be considered as security concerns regarding the deployment of this product (Bug[B], Vulnerability[V], Goodness[G], Informational[I]):

Finding	Description	Possible Mitigation(s)	Risk Level
B1	In /firewall_rules_edit.php line 503 & 517 has an if statement with "Identical sub-expressions on both sides of operator "&&""[6] which could lead to a vulnerability. CVE-2014-1266 is one such case that is attributed to this.	Remove duplicate entry	Low – 3.8[7]
G1	It was observed that there were 132 instances of switch statements without a declared default case.[8] /etc/inc/aws/Guzzle/Http/EntityBody.php /etc/inc/aws/Guzzle/Http/Message/Request.php /etc/inc/aws/Guzzle/Plugin/Cache/CachePlugin.php /etc/inc/aws/Guzzle/Plugin/Oauth/OauthPlugin.php /etc/inc/aws/Guzzle/Service/Command/LocationVisitor /Request/AbstractRequestVisitor.php /etc/inc/config.console.inc /etc/inc/filter.inc /etc/inc/gwlb.inc /etc/inc/interfaces.inc /etc/inc/ipsec.attributes.php /etc/inc/ipsec.inc /etc/inc/led.inc /etc/inc/meta.inc /etc/inc/openvpn.attributes.php /etc/inc/openvpn.inc /etc/inc/pfsense-utils.inc /etc/inc/radius.inc /etc/inc/services.inc	Although not necessary, if developers choose not to use a default case they would need to ensure that there are no cases that have not been considered. By adding the default case statements provides mitigation of all un-accounted conditions.	Informational

[6] MSC12-C. Detect and remove code that no effect or is never executed.
[7] CVSS Vector CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L
[8] CWE-478. Missing Default Case in Switch Statement.

	/etc/inc/shaper.inc /etc/inc/simplepie/simplepie.inc /etc/inc/smtp.inc /etc/inc/system.inc /etc/inc/upgrade_config.inc /etc/inc/vpn.inc /etc/inc/vslb.inc /etc/inc/xmlrpc_client.inc /usr/local/bin/3gstats.php /usr/local/bin/dhcpd_gather_stats.php /usr/local/lib/php/build/run-tests.php /usr/local/www/classes/Form/Input.class.php /usr/local/www/classes/Form/IpAddress.class.php /usr/local/www/csrf/csrf-magic.php /usr/local/www/diag_arp.php /usr/local/www/diag_backup.php /usr/local/www/diag_dns.php /usr/local/www/diag_edit.php /usr/local/www/diag_gmirror.php /usr/local/www/diag_packet_capture.php /usr/local/www/diag_testport.php /usr/local/www/easyrule.php /usr/local/www/firewall_aliases.php /usr/local/www/firewall_rules.php /usr/local/www/firewall_shaper_queues.php /usr/local/www/interfaces_ppps_edit.php /usr/local/www/interfaces.php /usr/local/www/load_balancer_monitor_edit.php /usr/local/www/load_balancer_virtual_server_edit.php /usr/local/www/pkg_edit.php /usr/local/www/rrd_fetch_json.php /usr/local/www/status_carp.php /usr/local/www/status_dhcp_leases.php /usr/local/www/status_dhcpv6_leases.php /usr/local/www/status_lb_pool.php /usr/local/www/status_ntpd.php /usr/local/www/status_services.php /usr/local/www/vpn_ipsec_phase1.php /usr/local/www/vpn_ipsec_phase2.php /usr/local/www/widgets/widgets/ipsec.widget.php /usr/local/www/wizard.php /usr/local/www/wizards/openvpn_wizard.inc /usr/local/www/xmlrpc.php		
I1	In /etc/inc/config.console.inc the function “Set_networking_interfaces_ports” (95) has a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is maintainability of these functions. Refactoring code into shorter functions will not necessarily reduce the potential for defects – it can raise the risk of mistakes	Informational

		in the interface between calling and called functions. Refactoring, when performed with care, can result in more maintainable code.	
I2	In /etc/inc/filter.inc the functions “filter_configure_sync” (81) “filter_nat_rules_generate” (137) “filter_generate_user_rule” (170) “fileter_rules_generate” (137) have a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I3	In /etc/inc/gwlb.inc the function “return_gateways_array” (100) has a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I4	In /etc/inc/interfaces.inc the functions "interface_ppps_configure" (118) "interface_wireless_configure" (75) "interface_configure" (85) have a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I5	In /etc/inc/led.inc the function “char_to_morse” (110) Has a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is	Informational

		recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	
I6	In /etc/inc/openvpn.inc the function "openvpn_reconfigure" (123) has a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I7	In /etc/inc/services.inc the functions "services_radvd_configure" (84) "services_dhcpdv4_configure" (194) "services_dhcpdv6_configure" (91) have a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I8	In /etc/inc/simplepie/simplepie.inc the functions "get_enclosures" (322) "encoding" (1082) have a high cyclomatic complexity rating.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I9	In /etc/inc/smtp.inc the functions "ConnectToHost" (81) "Connect" (70) have a high cyclomatic complexity rating	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is	Informational

		recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	
I10	In /etc/inc/system.inc the function "system_ntp_configure" (83) has a high cyclomatic complexity.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I11	In /etc/inc/upgrade_config.inc the function "upgrade_046_to_047" (75) has a high cyclomatic complexity.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I12	In /etc/inc/vpn.inc the function "vpn_ipsec_configure" (330) has a high cyclomatic complexity.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational
I13	In /usr/local/www/wizards/traffic_shaper_wizard_dedicated.inc the function "apply_all_chosen_items" (169) has a high cyclomatic complexity.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is	Informational

		recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	
I14	In /usr/local/www/wizards/traffic_shaper_wizard_multi_all.inc the function "apply_all_chosen_items" (171) Has a high cyclomatic complexity.	A cyclomatic complexity rating is not considered flaw or vulnerability but the concern is when these functions require updates. If the function is overly complex it is easier to introduce more bugs/regressions. It is recommended that these functions get split up into multiple functions instead of a single, all-encompassing function.	Informational

Configuration

The engagement team observed in php.ini that expose_php=off, magic_qutoes_gpc=off and as mentioned above register_globals was not present since it was deprecated in PHP 5.3.0 and completely removed in PHP 5.4.0, the version under review is currently using PHP 5.6.23. Additionally, it was observed that PHP was configured with the following flags of note:

- --disable-all – A build that only contains a minimum of extensions included in the build.
- --enable-fpm – A process manager for processing requests by spawning separate processes
- --with-fpm-user=www – Setting the PHP-FPM service to run as user “www”
- --with-fpm-group=www - Setting the PHP-FPM service to run as group “www”
- --fstack-protector – Provides additional protection against buffer overflows.

It was observed that the user “www” is also configured to not allow login and that the file system permissions on the web-root and included paths have been set to user “root” and group “wheel” with read/write only for owner and read for group and other. As a result, the web server process does not have write access to the web-root directory tree. This follows the principle of least privileges when deploying web services and provides an added layer of security via file system access control and authorization.

The engagement team identified an opportunity to potentially enhance security in the management page which allows for execution of Unix shell commands. The page is accessible only to privileged users, and no security flaw was found which would permit commands to be run by non-privileged users. Although PHP-FPM is run as "www" user, shell execution is passed to the ngnix process which is run as "root" user there could be a potential for abuse. The command line execution capability could allow a malicious user with access to this page the ability to damage the appliance. By creating a filter mechanism which only allowed specific commands, it should be possible to offer a command interface

which would be limited against executing arbitrary dangerous commands (Similar to the use of the 'sudo' utility's command filtering mechanism).

File Comments

The engagement team observed the following code comments of note that should be addressed:

- In the file /etc/inc/authgui.inc line 85 that there is a "FIXME" comment mentioning that a POST logout should be used instead of GET, there is a potential to be abused.
- In the file /usr/local/www/vpn_ipsec_profile.php on line 594 that there is a hard coded password "iOSPasswd123". Hard coded passwords should be avoided.
- In the file /usr/local/www/rrd_fetch_json.php on line 71 there is a TODO statement mentioning validation checks for several variables being assigned values, this should be addressed.
- In the file /usr/local/www/status_monitoring.php on line 798 there is a TODO statement mentioning validation checks for several variables being assigned values, this should be addressed.

Other Observations

The engagement team made an observation about the export capabilities in the system. If a configuration backup is made without the encryption option, then it could be edited maliciously, if it is not stored in a secure manner, e.g., allowing someone to create fictitious users with full privileges.

The team tested an export performed with a limited privilege account that only had access to the backup page. In larger organizations a Backup Operator will generally have the responsibility of taking the backup, but responsibility for restoration may be assigned to different personnel. Currently, any user with backup privileges also has restore privileges, and through exporting a non-encrypted backup and editing it, could restore it, to gain super user access, overtly, or in the form of a hidden account. The "Insider threat" scenario could be considered a minor threat but an infected internal host with C&C malware could leverage the backup mechanism to gain a foothold in the firewall system. There are three recommendations that the review team considers as mitigation strategies for this type of scenario:

1. Provide a more granular privilege on configuration export by separating the backup and restore pages thus allowing for separation of duties.
2. Provide comments in deployment guides advising customers to ensure that this scenario is mitigated by only allowing "trusted" individuals access the current configuration page.
3. Change the default setting of exporting configuration files to be in encrypted.

When the engagement team reviewed the cryptographic components of the TOE it was observed that good cryptographic security practices were applied in the ciphers selection. Data on the pfSense security appliance is stored using AES-256-CBC to secure information. The results of the scanning tools indicate that TLS v1.1 and TLS v1.2 are both supported. No known attacks or vulnerabilities were discovered for exploitation during the timeframe of the review period. ISG does recommend that unless backward compatibility is of concern it would be reasonable to disable obsolete ciphers by default, preventing the possibility of downgrade attacks.

System upgrades are often a use case which requires extensive review, as compromising the update process can compromise the entire system. The reviewed version of pfSense is using the FreeBSD pkg repository mechanism of distributing a sha-256 hash ('fingerprint') of the RSA public key corresponding to the private key used to sign the software repository. While this is not as strong as distributing the RSA public key itself, it is not currently feasible to construct a public RSA key which intentionally collides with the sha-256 hash of the pfSense RSA public key. It will be worthwhile monitoring the evolution of upgrade protection mechanisms available in FreeBSD in case stronger ones become available later on.

7.3.2 Third Party Components

7.3.2.1 BZip2 1.0.6

Finding	Description	Possible Mitigation(s)	Risk Level
CVE-2016-3189	Partial Use-after-free vulnerability in bzip2recover in bzip2 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted bzip2 file, related to block ends set to before the start of the block.	At this time there are no patched versions available from the vendor. When a patched version is released update this package in accordance to in-house release schedule.	Medium – 6.5[9]

7.3.2.2 cURL 7.49.1

Finding	Description	Possible Mitigation(s)	Risk Level
CVE-2016-7167	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.	Update cURL to version 7.50.3 or greater.	Critical – 9.8[10]
CVE-2016-7141	cURL and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.	Update cURL to version 7.50.2 or greater.	High – 7.5[11]
CVE-2016-5421	Use-after-free vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or	Update cURL to version 7.50.1 or greater.	Critical – 9.8[12]

[9] CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
[10] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
[11] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
[12] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

	possibly have unspecified other impact via unknown vectors.		
CVE-2016-5420	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.	Update cURL to version 7.50.1 or greater.	High – 7.5[13]
CVE-2016-5419	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.	Update cURL to version 7.50.1 or greater.	High – 7.5[14]

7.3.2.3 OpenSSL 1.0.1s

Finding	Description	Possible Mitigation(s)	Risk Level
CVE-2016-6306	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.	Update OpenSSL to version 1.0.1u or greater.	Medium – 5.9[15]
CVE-2016-6304	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.	Update OpenSSL to version 1.0.1u or greater.	High - 7.5[16]
CVE-2016-2176	The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.	Update OpenSSL to version 1.0.1t or greater.	High – 8.2[17]
CVE-2016-2109	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL	Update OpenSSL to version 1.0.1t or greater.	High - 7.5[18]

[13] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
[14] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
[15] CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
[16] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
[17] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
[18] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

	before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.		
CVE-2016-2107	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session, NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.	Update OpenSSL to version 1.0.1t or greater.	Medium – 5.9[19]
CVE-2016-2106	Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.	Update OpenSSL to version 1.0.1t or greater.	High – 7.5[20]
CVE-2016-2105	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.	Update OpenSSL to version 1.0.1t or greater.	High – 7.5[21]

7.3.2.4 Libxml2 2.9.3

Finding	Description	Possible Mitigation(s)	Risk Level
CVE-2016-4449	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4	Update Libxml2 to version 2.9.4 or greater.	High – 7.1
CVE-2016-4448	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.	Update Libxml2 to version 2.9.4 or greater.	Critical – 9.8
CVE-2016-4447	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-	Update Libxml2 to version 2.9.4 or greater.	High – 7.5

[19] CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
[20] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
[21] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

	based buffer underread and application crash) via a crafted file.		
CVE-2016-3705	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth.	Update Libxml2 to version 2.9.4 or greater.	High – 7.5
CVE-2016-3627	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier.	Update Libxml2 to version 2.9.4 or greater.	High – 7.5

7.3.2.5 Readline 5.2

Finding	Description	Possible Mitigation(s)	Risk Level
CVE-2014-2524	The _rl_tropen function in util.c in GNU readline before 6.3 patch 3 allows local users to create or overwrite arbitrary files via a symlink attack on a /var/tmp/rltrace.[PID] file.	Update Readline to 6.3 patch 3 or greater.	Medium – 4.4[22]

7.3.2.6 PHP 5.6.23

Finding	Description	Possible Mitigation(s)	Risk Level
CVE-2016-6297	Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.	Update PHP to version 5.6.24/7.0.9 or greater.	High – 8.8[23]
CVE-2016-6296	Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.	Update PHP to version 5.6.24/7.0.9 or greater.	Critical – 9.8[24]
CVE-2016-6295	ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows	Update PHP to version 5.6.24/7.0.9 or greater.	Critical – 9.8[25]

[22] CVSS 3 score based on CVE CVSS 2 reference CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L
[23] CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
[24] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
[25] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

	remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.		
CVE-2016-6294	The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.	Update PHP to version 5.6.24/7.0.9 or greater.	Critical – 9.8[26]
CVE-2016-6292	The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.	Update PHP to version 5.6.24/7.0.9 or greater.	Medium – 6.5[27]
CVE-2016-6291	The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.	Update PHP to version 5.6.24/7.0.9 or greater.	Critical – 9.8[28]
CVE-2016-6290	ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.	Update PHP to version 5.6.24/7.0.9 or greater.	Critical – 9.8[29]

[26] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
[27] CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
[28] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
[29] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2016-6289	Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.	Update PHP to version 5.6.24/7.0.9 or greater.	High – 7.8[30]

7.3.2.7 Simplepie 1.3.1

Finding	Description	Possible Mitigation(s)	Risk Level
	In /etc/inc/simplepie/simplepie.inc has 24 instances of duplicate case statements within the same switch function[31] which could lead to bugs or vulnerabilities.	Upgrade to Simplepie 1.4.3 or greater.	Low – 3.1[32]

7.3.2.8 Third Party Components

The following are the third party components that did not have any known vulnerabilities or weaknesses against the observed versions discovered by the engagement team as of authoring this report.

Name	Version
FreeBSD	10.3 r5
Ngnix	1.10.1
PHP-FPM	5.6.23
Zlib	1.2.8
Libxml	2.9.3
Libmcrypt	2.5.8
MYSQLND	5.0.11
PCRE	8.3.9
SQLite	3.13.0
DOM/XML	20031129
JSON	1.2.1
OpenLDAP	2.4.44
Libmbfl	1.3.2
Radius	1.3.0
RRD Library	1.6.0

[30] CVSS Vector CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L
[31] MSC12-C. Detect and remove code that no effect or is never executed.
[32] CVSS Vector CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L

SSH2	1.17
LibSSH2	1.7.0
Suhosin	0.9.38
Xdebug	2.4.0
ZMQ extension	1.1.3
Libzmq	4.14
OpenVPN	2.3.11
Zend Framework	2.6.0

8 Conclusion

The ISG security assessment of Netgate XG-2758-1U pfSense Security Appliance identified some potential security concerns, none of which were deemed to be of a high or critical severity. However, as a caveat to this statement, the following point should be noted:

- It should be noted in the pfSense documentation that there is a potential for abuse regarding backup/restore of configuration emphasizing potential mitigation or the reliance on trust in users with access to the backup/restore functionality.

It is important to note that a security assessment is a static document that assesses risk variables at a fixed point in time for a given array of assets in a set configuration. Conversely, business requirements are not static, making the programs, services and the associated assets change over time; which in turn change the threats that may affect them. New vulnerabilities are also discovered on a regular basis, especially with respect to complex information technologies. Therefore, in an inherently dynamic environment, continuous risk management is essential. The overall opinion of the engagement team is that the Netgate XG-2758-1U pfSense security appliance is well designed, robust and secure security appliance with a large community behind it making this product an easy choice to recommend for businesses of any size.

9 Addendum

At the time that this report was completed, Rubicon Communications has been working on the next release of pfSense (version 2.3.3). The following items from this report have been addressed on the 2.3.3 development branch of their software, and this was confirmed by further review by the ISG evaluation team.

Finding	Description	Possible Mitigation(s)	Risk Level
B1	In /firewall_rules_edit.php line 503 & 517 has an if statement with "Identical sub-expressions on both sides of operator "&&""[33] which could lead to a vulnerability. CVE-2014-1266 is one such case that is attributed to this.	Remove duplicate entry	Low – 3.8[34]

Vulnerable component	Affected Version	Updated Version
curl	7.49.1	7.51.0_1
Libxml2	2.9.3	2.9.4
Php56	5.6.23	5.6.28
Simplepie	1.3.1	1.4.3

[33] MSC12-C. Detect and remove code that no effect or is never executed.
[34] CVSS Vector CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L