WatchGuard AP - Remote Code Execution

Security Advisory

SECURITY

Date 1/05/2018

Version: 1.0

Table of Contents

1. Document Control

1.1. Document Information

Title	WatchGuard AP - Remote Code Execution - Security Advisory
Document Filename	ZX Security Advisory - Watchguard Access Points - Multiple Vulnerabilities.docx

1.2. Revision Control

Version	Date Released	Pages Affected	Author	Description
1.0	01/05/2018	All	Stephen Shkardoon	Initial release

2. Background

2.1. Introduction

ZX Security identified several major vulnerabilities within WatchGuard Access Point devices that can be chained together to gain pre-authenticated remote code execution on the devices.

2.2. Vendor notification

The vendor has provided several articles regarding the identified issues:

- https://watchguardsupport.secure.force.com/publicKB?type=KBSecurityIssues&SFDCID=kA62A0000000LIy
- https://www.watchguard.com/wgrd-blog/new-firmware-available-ap100ap102ap200ap300-security-vulnerability-fixes

2.3. Affected devices

All issues are present on the following devices:

- AP100
- AP102
- AP200

Additionally, all issues except for the hardcoded access credentials are present on the following additional devices:

- AP300

2.4. Disclosure Timeline

ZX Security would like to commend the prompt response and resolution of these reported issues by the vendor.

Vendor notification:	April 04, 2018
Vendor response:	April 06, 2018
Firmware update released to public:	April 13, 2018

3. Technical Findings

3.1. Hard-coded credentials

CVE-2018-10575

A hard-coded user exists in /etc/passwd. The vendor has requested the specific password and hash be withheld until users can apply the patch.

There is no way for a user of the access point to change this password. An attacker who is aware of this password is able to access the device over SSH and pivot network requests through the device, though they may not run commands as the shell is set to /bin/false.

3.2. Hidden authentication method in web interface allows for authentication bypass

CVE-2018-10576

The standard authentication method for accessing the webserver involves submitting an HTML form. This uses a username and password separate from the standard Linux based /etc/passwd authentication.

An alternative authentication method was identified from reviewing the source code whereby setting the HTTP headers AUTH_USER and AUTH_PASS, credentials are instead tested against the standard Linux /etc/passwd file. This allows an attacker to use the hardcoded credentials found previously (see 1. Hard-coded credentials) to gain web access to the device.

An example command that demonstrates this issue is:

```
curl https://watchguard-ap200/cgi-bin/luci -H "AUTH_USER: admin" -H "AUTH_PASS: [REDACTED]" -k -v
```

This session allows for complete access to the web interface as an administrator.

3.3. Hidden "wgupload" functionality allows for file uploads as root and remote code execution

CVE-2018-10577

Reviewing the code reveals file upload functionality that is not shown to the user via the web interface. An attacker needs only a serial number (which is displayed to the user when they login to the device through the standard web interface and can be retrieved programmatically) and a valid session.

An example request to demonstrate this issue is:

```
res = send_request_cgi({
       'method'    => 'POST',
       'uri'       => "/cgi-bin/luci/;#{stok}/wgupload",
       'headers' => {
         'AUTH_USER' => 'admin',
         'AUTH_PASS' => '[REDACTED]',
       },
       'cookie'        =>  "#{sysauth};  serial=#{serial};  filename=/www/cgi-bin/payload.luci;
md5sum=fail",
       'data'     => "#!/usr/bin/lua
os.execute('touch /code-execution');
  })
```

An attacker can then visit the URL http://watchguard-ap200/cgi-bin/payload.luci to execute this command (or any other command).

3.4. Change password functionality incorrectly verifies old password

CVE-2018-10578

The change password functionality within the web interface attempts to verify the old password before setting a new one, however, this is done through AJAX. An attacker is able to simply modify the JavaScript to avoid this check or perform the POST request manually.

4. Further details & Metasploit module

ZX Security will be releasing a Metasploit module which automates exploitation of this chain of vulnerabilities. This has been delayed till 30 days after the initial patch was made available to ensure users are able to patch their devices.

The module and the hardcoded password will be released on May the 14th 2018.

ZX Security Limited
Level 1, 50 Manners St
Wellington, New Zealand