SECURITY ADVISORY

Netgear WNR2000v5
UNAUTHENTICATED REMOTE CODE EXECUTION

MAXIME PETERLIN
23/05/2017
CVE-2017-6862
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

<table>
<thead>
<tr>
<th>DATE</th>
<th>EVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>16/12/2016</td>
<td>First contact with the Netgear Security Team.</td>
</tr>
<tr>
<td>23/12/2016</td>
<td>Acknowledgement from Netgear.</td>
</tr>
<tr>
<td>06/04/2017</td>
<td>Security advisory sent to Netgear for review.</td>
</tr>
<tr>
<td>14/04/2017</td>
<td>Security advisory reviewed by Netgear.</td>
</tr>
<tr>
<td>23/05/2017</td>
<td>Security advisory released.</td>
</tr>
</tbody>
</table>
2. TECHNICAL DETAILS

2.1. VULNERABILITY DETAILS

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.

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

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

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

Figure 5 - Remote code execution
3. REFERENCES

- **NETGEAR**, 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