Sense of Security	Authorisation. Jason Edelstein
	Release date. 20 September 2011.

Sense of Security – Security Advisory – SOS-11-011.

NETGEAR Wireless Cable Modem Gateway CG814WG Auth Bypass and CSRF.

20 September 2011.

NETGEAR Wireless Cable Modem Gateway CG814WG Auth Bypass and CSRF - Security Advisory - SOS-11-011

Release Date.	20-Sep-2011
Last Update.	-
Vendor Notification Date.	22-Mar-2011
Product.	NETGEAR Wireless Cable Modem Gateway CG814WG
Affected versions.	Hardware 1.03, Software V3.9.26 R14 verified and possibly others
Severity Rating.	High
Impact.	Authentication bypass and Cross Site Request Forgery
Attack Vector.	Remote without authentication
Solution Status.	Upgrade to R15 (by contacting NETGEAR)
CVE reference.	Not yet assigned

Details.

The NETGEAR Wireless Cable Modem Gateway CG814WG is supplied by ISP's as customer premises equipment within Australia and abroad. It is a centrally managed ISP solution whereby each ISP's devices run a customised firmware and configuration changes and updates can be pushed out as required.

Basic authentication is used as the primary and only authentication mechanism for the administrator interface on the device. The basic authentication can be bypassed by sending a valid POST request to the device without sending any authentication header. The response from the device sends the user to another page that requests basic authentication, however at this point the request has already been processed.

An example of attacks using the basic authentication bypass may include changing the admin password or enabling the remote admin interface (Internet facing).

Additionally, due to the lack of CSRF protection in the web application, the bypass attack can be coupled with CSRF to have a victim enable the remote admin interface to the Internet, where an attacker can then use the bypass attack again across the remote admin interface to reset the admin password and access the device. This attack is possible when targeting a victim that is behind the NETGEAR device on the same segment as the web administrator interface whom has browsed to a malicious site containing the CSRF attack.

NETGEAR was notified of this vulnerability on 22 March 2011, but we never received a response or acknowledgement of the issue or fix. Sense of Security notified local ISP's and it was escalated by a local ISP who worked with NETGEAR to develop and test an update. Sense of Security was never provided an opportunity to validate the fixes in the latest firmware version. Given the severity of the issue it would be prudent for NETGEAR to notify and supply an update to all of its customers.

Proof of Concept.

By embedding the below HTML in a website and having a victim browse to the website the remote management interface to the Internet would be enabled. An attacker could then use one of the hardcoded passwords for the device to access it, or use a basic authentication bypass to change the admin password. Alternatively, the attacker could conduct a CSRF attack that implements two POST requests to have the remote admin interface enabled, and the admin password changed.

The example here is a basic proof of concept, more complex examples which include JavaScript redirects to mask the basic authentication pop-up would be more stealthy.

```
<html>

<head></head>

<body onLoad=javascript:document.form.submit()>

<form action="http://192.168.0.1/goform/RgRemoteManagement" method="POST" name="form">

<input type="hidden" name="NetgearRmEnable" value="0x01">

<input type="hidden" name="NetgearRmPortNumber" value="1337">

<input type="hidden" name="NetgearUserLevel" value="1">

</form>

</body>

</html>
```

Solution.

Ask your ISP to obtain the latest firmware from NETGEAR and deploy it to your device.

Discovered by.

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-11-011.pdf

Other Sense of Security advisories can be found at:

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