
Vulnerability Summary

May 2004

Paul Asadoorian
Lead IT Security Specialist
Brown University

Vulnerabilities

- NetGear WG602 backdoor account
- Oracle SQL Injection vulnerabilities
- ISC DHCP Multiple Bugs
- Special Feature: Digital Certificates

NetGear WG602 backdoor account

- Netgear Wireless Gateway, model WG602
- Backdoor account exists
 - Username: super
 - Password: 5777364
- Password is phone number of Taiwanese manufacturer
 - www.zcom.com.tw/contact.htm



NetGear WG602 backdoor account

- Only firmware version verified to be vulnerable is 1.5.67
- Version 1.7.14 is reportedly vulnerable, but different username and password
- Current Firmware version is **1.7.15**
- This version does not appear to be vulnerable

NetGear WG602 backdoor account

- Upgrade your firmware
- Change the default administrative password
- Devices are targets too!

NetGear WG602 backdoor account

- Netgear Support page
 - http://kbserver.netgear.com/products_automat ic/WG602v1.asp
- Advisories:
 - <http://www.security.nnov.ru/search/document. asp?docid=6294>
 - <http://www.securityfocus.com/bid/10459/>

Oracle SQL Injection vulnerabilities

- Affected Products:
 - Oracle Applications 11.0 (all releases)
 - Oracle E-Business Suite 11i, 11.5.1-11.5.8
- What is SQL Injection?

Oracle SQL Injection vulnerabilities

- Access database through web server
- Two Kinds:
 1. Steal data (i.e. student's SSN numbers)
 2. Gain remote access to database server
 - Database must support OS commands

Oracle SQL Injection vulnerabilities

- Manipulates the URL to send commands to the database
- SQL commands will return data
- OS commands are used to plant backdoor and other malicious activity

Oracle SQL Injection vulnerabilities

- Patch Available
- Follow good coding practices
- Advisories:
 - <http://www.us-cert.gov/cas/techalerts/TA04-160A.html>
 - <http://otn.oracle.com/deploy/security/pdf/2004alert67.pdf>

ISC DHCP Multiple Bugs

- ISC DHCP versions 3.0.1rc12 and 3.0.1rc13
- Two buffer overflows exist
- Cause DoS
- Remote exploit may be possible

ISC DHCP Multiple Bugs

- One vulnerability affects all platforms
- The other is limited to:
 - AIX
 - AlphaOS
 - Cygwin32
 - HP-UX
 - Irix
 - Linux
 - NextStep
 - SCO
 - SunOS 4
 - SunOS 5.5
 - Ultrix

ISC DHCP Multiple Bugs

- Advisories:
 - <http://www.us-cert.gov/cas/techalerts/TA04-174A.html>
- Vulnerability Notes:
 - <http://www.kb.cert.org/vuls/id/317350>
 - <http://www.kb.cert.org/vuls/id/654390>

Digital Certificates

- What are they?
- Why do you need them?
- How do I set them up?

Digital Certificates

- Sign & encrypt your email
- Verifies that email really comes from you
- Share secrets with your friends
- Best of all, its free!

Digital Certificates

- Step 1 – Request a Digital Certificate
- Step 2 – Installing your digital certificate
- Step 3 – Using your digital certificate to sign email

Digital Certificates

- Thawte offers free personal digital certificates
 - <https://www.thawte.com/products/index.html>
Go to Bottom → Personal Email Certificates
- Fill out some basic information
- Creates an account with Thawte for all your Digital Certificate needs

Digital Certificates

New Registration in Thawte's Personal Cert System - Mozilla Firefox

information and involves an exhaustive enquiry by us. **Please complete this enrollment ONCE only.**

If you are likely to enter characters that are not ASCII (ie accented characters) on this page or subsequent pages of the enrollment process, please choose a character encoding or charset from the drop-down list box below. If you are not sure what charset to choose click [here](#) to get a list of recommended charsets for languages. The default charset choice is the recommended charset for your browser language preference.

Charset For Text Input:

Name And Nationality
Please note that you need to be 13 years or older to enroll in the personal cert system
Please complete the form below:

Surname or Family Name

First Names or Given Names

Date Of Birth
Please give your date of birth.
You need to specify the full year, including century. For example, "1973" or "1942".

Nationality

Digital Certificates

- Once process is complete you will get email
- Must use the same email you entered previously
- Click link and confirm the request

Digital Certificates

“According to our records you have just submitted a new email address for verification by Thawte. By following these instructions you will prove that you can read email sent to paul@pauldotcom.com.”

Digital Certificates

- Your request will be processed
- Wait for another email saying your certificate is ready
- Sometimes only takes 10-15 minutes, check your email

Digital Certificates

Follow link sent in email:

“This is an automated message to let you know that we have just issued your personal certificate. You can retrieve it at:

<https://www.thawte.com/cgi/personal/cert/deliver.exe?serial=XXXXXX>

Remember, you will need your Thawte ID and password to access the Personal Certification System. You also need to be running the same browser, on the same machine, logged in as the same user, as you were when you made the request.”

Digital Certificates

- Follow link and click “Install Certificate”
- Use Internet explorer
 - DOH! Doesn’t work in other browsers
 - It’s free though 😊
- To view, click “Tools → Internet Options → Content → Certificates...”

Digital Certificates

- Outlook Express should see the new certificate
 - Tools → Options → Security → Digital IDs...
- Compose new message, then click “Sign”
- Click okay to allow access to your private key

Digital Certificates

- To sign or not to sign
- Use it especially for important emails
 - Email to all users
 - Proposals
- Help:
 - <http://www.thawte.com/support/email/index.html>

Article Of The Month

“Time to Dump Internet Explorer”

<http://www.securityfocus.com/columnists/249>

"IE is a buggy, insecure, dangerous piece of software, and the source of many of the headaches that security pros have to endure..."

/* The End */

Essential Security Links

<http://packetstormsecurity.nl/>

<http://www.security.nnov.ru/>

<http://www.cert.org>

<http://www.whitehats.com>

<http://rr.sans.org>

<http://www.incidents.org>

<http://www.astalavista.com/>

<http://www.incidents.org>

<http://www.l0t3k.org/>



<http://www.securiteam.com/>