Sense of Security	Authorisation. Jason Edelstein
	Release date. 5 March 2010.

Sense of Security – Security Advisory – SOS-10-002.

Apache 2.2.14 mod_isapi Dangling Pointer Vulnerability.

5th March 2010.

Apache mod_isapi Dangling Pointer Vulnerability - Security Advisory - SOS-10-002

Release Date.	5-Mar-2010
Last Update.	-
Vendor Notification Date.	9-Feb-2010
Product.	Apache HTTP Server
Platform.	Microsoft Windows
Affected versions.	2.2.14 verified and possibly others
Severity Rating.	High
Impact.	Remote code execution with the privileges of the SYSTEM user
Attack Vector.	Remote without authentication
Solution Status.	Upgrade to 2.2.15 (as advised by Apache)
CVE reference.	CVE-2010-0425

Details.

The Apache HTTP Server, commonly referred to as Apache, is a popular open source web server software. mod_isapi is a core module of the Apache package that implements the Internet Server extension API. The extension allows Apache to serve Internet Server extensions (ISAPI .dll modules) for Microsoft Windows based hosts.

By sending a specially crafted request followed by a reset packet it is possible to trigger a vulnerability in Apache mod_isapi that will unload the target ISAPI module from memory. However function pointers still remain in memory and are called when published ISAPI functions are referenced. This results in a dangling pointer vulnerability.

Successful exploitation results in the execution of arbitrary code with SYSTEM privileges.

Proof of Concept.

Proof of concept exploit code is available for this vulnerability. The payload will write a text file (sos.txt) to the Apache working directory demonstrating that code execution is possible. The code can be downloaded from the following link:

http://www.senseofsecurity.com.au/advisories/SOS-10-002-pwn-isapi.cpp

Furthermore, a video demonstrating the exploitation of this vulnerability using a bind shell has been created. It can be viewed at the following link:

http://www.senseofsecurity.com.au/movies/SOS-10-002-apache-isapi.mp4

Solution.

Upgrade to the latest version of Apache HTTP Server (currently 2.2.15).

Discovered by.

Brett Gervasoni 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 countries largest organisations.

Sense of Security Pty Ltd

Level 3, 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/consulting/penetration-testing
E: info@senseofsecurity.com.au
Twitter: ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-10-002