Response to Hacks in the News

1. **Date and original announcement of Hack/vulnerability**: June 25, 2002
http://httpd.apache.org/info/security_bulletin_20020620.txt
http://www.cert.org/advisories/CA-2002-17.html

2. The Attack name: **Apache chunked transfer-encoding vulnerability**

Attack target:
Execution of commands remotely (Apache 1.3), Denial of service (Apache 2.0).

Attack Description:
Using a bug in the way Apache handles requests with chunked transfer-encoding (a method which allows sending requests in chunks, as opposed to a single bulk), it is possible to cause a stack overflow (on Apache 1.3) that can lead to remote command execution. On Apache 2.0 the bug will cause the current (child) process to stop (and a new one has to be created to replace it), which inflicts excessive CPU load on the machine. Sending multiple such results effectively triggers a denial of service condition on the server.

Details on Method of Attack/Technique:
The attack involves using a very rare HTTP header in the request - it will contain (among the HTTP headers):

Transfer-Encoding: chunked

This header itself is legitimate. The exploitation code (for Apache 1.3 remote command execution) is placed in the request's body, in the chunked encoding format. The stack overflow is caused by not following the format for chunked transfer-encoding body. This format dictates that each chunk is preceded by a hexadecimal number stating the length of the chunk following it. By providing overly large (> 2 to the power of 31) such numbers it is possible to trigger the stack overflow (probably due to signed/unsigned integer type mismatch). The chunk itself need not be excessively large.

A single HTTP request suffices to execute the attack (for the remote command execution).

Exploit code:
Available for Apache 1.3 on OpenBSD

Exploit code (courtesy of GOBBLES):
http://online.securityfocus.com/attachment/2002-06-25/apache-scalp.c
(remote command execution for Apache/1.3 on OpenBSD)

Typical Vulnerable System(s):
Remote command execution: Apache/1.3.24 and below, on operating systems: OpenBSD, FreeBSD, Solaris, Linux, Windows. Possibly vulnerable on Unix 64 bit operating systems as well.Denial of service: Apache/2.0.36 and below, probably on all operating systems.

History:
First public appearance in a message sent by ISS to BugTraq: June 17th, 2002 (without notifying the vendor first!)
However, the vulnerability was reported to the Apache Group earlier by David Litchfield of NGSSoftware

GOBBLES security (a team of hackers/researchers) also claim to have knowledge of this vulnerability for some time. They published a working exploitation code for Apache/1.3 on OpenBSD, and claim to have working code for several other operating systems.

The applicability of the exploitation was much debated, but apparently the exploitation code provided by GOBBLES demonstrated that the attack is realistic on common operating system.

Solution*: How Sanctum's AppShield can stop the attack*

AppShield
In AppShield 4.0 (and earlier versions), requests using chunked encoding are automatically filtered out by AppShield. AppShield will issue a 501 error page and block the request.