GHOST glibc gethostbyname()
Vulnerability CVE-2015-0235

Johannes B. Ullrich, Ph.D.
SANS Technology Institute
https://isc.sans.edu
Outline

• Background: gethostbyname()
• Who is at risk?
• How to mitigate the vulnerability?
• How to detect the attack?
• Are there exploits available?
• How soon do I need to patch?
Background: glibc and gethostbyname

- glibc: GNU C Library
- Part of Linux Standard Base
- Available for most (all?) operating systems including Windows
- gethostbyname() is an (old) standard C/POSIX function implemented by many libraries
gethostbyname()

• Part of Berkeley Sockets
• Converts hostname to IPv4 address
• Replaced by getaddrinfo(), but still widely used
• Doesn’t fully support IPv6
The Vulnerability

• Before converting a host name to an IP address, the function checks if the parameter is already an IP address.
• The function miscalculates the size needed to store the data.
• As a result, not enough memory is allocated and the buffer overflow happens.
Exploit

- Overly large hostname consisting of numbers and up to 3 ‘.’s
- Only 4 or 8 bytes can be overwritten
- These bytes can only be numbers or ‘.’, making exploit development difficult
Who is vulnerable

- glibc 2.2 (Nov 2000) – glibc 2.17 (May 2013)
- Debian 7
- Red Hat Enterprise Linux 6 & 7
- CentOS 6 & 7
- Ubuntu 12.04 (14 uses glibc 2.19)
- Most BSD variants (FreeBSD, OpenBSD, OS X) are NOT vulnerable
Software using gethostbyname()

- Any software initiating network connections
- Log processing
- Mail/Spam filtering
- Many servers
- Exceptions: Software using the more modern getaddrinfo() function
Mitigating the attack

- Patch!
- Patches are available for all current Linux distributions

$ /lib/libc.so.6

GNU C Library stable release version 2.12, [...] Compiled on a Linux 2.6.32 system on 2015-01-27.
• CentOS /lib/libc.so.6
• Ubuntu /usr/lib/x86_64-linux-gnu/libc.so
• OS X: not installed by default, but maybe with homebrew/macports

find / -name 'libc.so*'
Detecting an Attack

• Attack requires a gethostbyname() for an extraordinary long hostname that contains only numbers and up to 3 dots:

1212313.1341241234.134234.31341
(typically > 1000 digits, only numbers works too)
Network Detect

• You may see the lookup on the network IF the attack fails
• Lookup for “A” record
• Check recursive name server logs
• No Snort signature as of now
Likelihood of Exploit

• Exploit is tricky.
  Only up to 8 bytes available to execute code
  Code can only contain digits and .
• Qualys provided quite a bit of detail in its advisory, showing DoS exploits against various software
• Claims to have exploit for Exim
Exploit Availability

- Qualys announced that they will release the Exim exploit “soon”
- Expect others to work hard on exploit development
- Lots of detail available
- Likely some exploit going to be available this week.
Summary

• This is a critical vulnerability for systems using the glibc function `gethostbyname()`
• Detection is possible but tricky
• Patch affected systems THIS WEEK
Thanks!

Questions:

jullrich@sans.edu
handlers@isc.sans.edu

https://isc.sans.edu/contact.html
You can find a PDF and PowerPoint file for this presentation at

https://isc.sans.edu/presentations