Tech - On - Tap

Monthly E-Journal

Dept. of. MCA

Month: January Issue: 1 Year: 2015

Student Coordinator

Anupama NC
Arfa Samreen
Aynaz Kauser S
Deenamol Jose
Deepika
Hamsalekha M

Staff Coordinator

Swarnamugi M

GHOST, A CRITICAL LINUX SECURITY HOLE, IS REVEALED

Researchers at cloud security company Qualys have discovered a major security hole, GHOST (CVE-2015-0235), in the Linux GNU C Library (glibc). This vulnerability enables hackers to remotely take control of systems without even knowing any system IDs or passwords. Qualys alerted the major Linux distributors about the security hole quickly and most have now released patches for it. Josh Bressers, manager of the Red Hat product security team said in an interview that, "Red Hat got word of this about a week ago. Updates to fix GHOST on Red Hat Enterprise Linux (RHEL) 5, 6, and 7 are now available via the Red Hat Network."

This hole exists in any Linux system that was built with glibc-2.2, which was released on November 10, 2000. Qualys found that the bug had actually been patched with a minor bug fix released on May 21, 2013 between the releases of glibc-2.17 and glibc-2.18. However, this fix was not classified as a security problem, and as a result, many stable and long-term-

support distributions are wide open today. Linux systems that are liable to attack include Debian 7 (Wheezy), RHEL 5, 6, and 7, CentOS 6 and 7 and Ubuntu 12.04. Besides Red Hat's fix, Debian is currently repairing its core distributions, Ubuntu has patched the bug both for 12.04 and the older 10.04, and I'm told the patches are on their way for CentOS.

The security hole can be triggered by exploiting glibc's gethostbyname functions. This function is used on almost all networked Linux computers when the computer is called on to access another networked computer either by using the /etc/hosts files or, more commonly, by resolving an Internet domain name with Domain Name System (DNS). To exploit this vulnerability, all an attacker needs to do is trigger a buffer overflow by using an invalid hostname argument to an application that performs a DNS resolution. This vulnerability then enables a remote attacker to execute arbitrary code with the permissions of the user running DNS. In short, once an attacker has exploited GHOST they may be capable of taking over the system.

"GHOST poses a remote code execution risk that makes it incredibly easy for an attacker to exploit a machine. For example, an attacker could send a simple email on a Linux-based system and automatically get complete access to that machine," said Wolfgang Kandek, Qualys's CTO in a statement. "Given the sheer number of systems based on glibc, we believe this is high severity vulnerability and should be addressed immediately. The best course of action to mitigate the risk is to apply a patch from your Linux vendor."

Unlike some security announcements, Kandek is not crying wolf. Qualys has developed a proof-of-concept in which simply sending a specially created e-mail to a mail server enabled them to create a remote shell to the Linux machine. According to Qualys, "This bypasses all existing protections (like ASLR, PIE and NX) on both 32-bit and 64-bit systems."

Seven things you need to know about the 'GHOST' vulnerability.

1. What is 'GHOST'?

'GHOST' is the name of a vulnerability recently found in one of the key components of Linux systems. The component is the Linux GNU C Library that is used by all Linux programs. The vulnerability has been found in a function of this library that is used to convert Internet host names to Internet addresses.

If an attacker found vulnerable software and a way to transfer a properly crafted host name up to this function, then theoretically the attacker could take over the control of the system.

2. How widespread is it?

This vulnerability affects almost all major Linux distributions, except a few such as Ubuntu 14.04. Millions of servers on the Internet contain this vulnerability. What does it mean? It means that the vulnerability exists on servers but there should be certain conditions met to render the server remotely attackable. According to Qualys' report, they have found an email server software called Exim that is remotely exploitable.

There is no recent and full deployment share report showing how many public Exim servers are on the Internet, however it has a measurable "market" share but according to some old reports its maximum just few percent. Note that to have an exploitable Exim-based email server one has to configure extra security checks for the HELO and EHLO commands of the SMTP protocol.

Fortunately Qualys found that many well-known Linux-based web, email and other server software are not affected by this vulnerability like Apache, nginx, OpenSSH, syslog-ng.
So we can say that apart from the fact that the vulnerability could be found on many servers, actually the remotely attackable share of these servers is low.

3. How can I secure my Exim email server?

First of all deploy security fixes to all affected Linux servers as soon as possible. All major distributions have released security patches on the same day the security advisory published the vulnerability. Keep in mind that to make security patch effective all affected software has been restarted. Many distributions do this automatically during glibc update, but many of them leave this job for you.

Please make sure that your Exim server is restarted. This restart causes an SMTP service outage but normally this is only a few seconds and your email server users should not have any major issue because of this. If there was any ongoing SMTP connection – sending or receiving email – that would be aborted due to the restart and then the other side or the Exim will resend the email shortly.

In similar cases the possible impact of an unplanned outage is much lower than the possible impact of a successful attack.

4. Could an attacker do anything else than just take control of an email server?

There is no exact answer to this question. It depends on your deployment and configuration.
If you use Exim just for front-end server as a smart host then the attacker can have access to your emails. If your email system is separated, and you do not store any credentials – passwords, SSH private keys, etc. – on the affected servers, then the impact could be relatively low.

But if your Exim server hosts the mailboxes and/or has server software on it then the attacker can have access to your data and in worst case to your other systems also. If you suspect that your server is attacked successfully, remove the server from operation immediately, plug out all network connections and execute your emergency plan. If you do not have such an emergency plan then maybe the easiest and most secure way is to reinstall the whole system.

5. Are my Linux servers safe now?

If you deployed security patches quickly and you have checked that your server software was not affected and/or there is no sign of any attack, then you can sit back. However we don't have information on all software mainly we don't know how much 3rd party software is affected. For example many email security, anti-spam software process email headers and take every Received: header line and they try to resolve host names found in these headers to check them against bad IP databases. So theoretically, a specially crafted email message can contain exploit code.

Of course this is only a speculation, but it points out that we can never be cautious enough because sometimes the possible consequences of vulnerability cannot be predicted. It is better to take more attention to your servers, log files and web sites of your Linux distribution and also the web sites of vendors of any 3rd party software you use on your servers in the next few days to make sure that you do not miss anything important regarding this vulnerability.

6. Is there anything I can do to be prepared for future vulnerabilities?

If you just need to execute previously defined steps, such as updating your infrastructure, to make sure that your system is secure then you did a great job as you prepared. However existing processes and infrastructure can always be improved. Take this time and think about your systems and processes. Is there a faster way to deploy security fixes? Is there any unnecessary/unused service that you can shut down to minimize attack surface?

7. What should I do as an Internet user?

You cannot do much. You are unlikely to be affected by this vulnerability.

There is a very small chance that an attacker could send you a fake email or catch your email via a hacked email server or access your personal information stored on a hacked server but the probability is low enough that you should not be worried.

Deenamol Jose
I Year MCA

FIVE PEN PC TECHNOLOGY

Introduction:

Imagine a world where everybody can use modern IT without being an expert. Imagine using only pen and paper to send-mails and SMS. Pen-style Personal Networking Gadget is computers in the shape of different pens each having a function of its own and when combined together give us the usage of a full-blown computer. It is a computer broken apart into pieces. At the 2003 ITU Telecom World exhibition held in Geneva, the Tokyo-based NEC Corporation displayed a conceptual $30,000 prototype of P-ISM. It is simply a new invention in computer and it is associated with communication field. Surely this will have a great impact on the computer field.

What is P-ISM?

When writing a quick note, pen and paper are still the most natural to use. The 5 pen pc technology with digital pen makes it possible to get a digital copy of handwritten information, and have it sent to digital devices via Bluetooth. P-ISM (Pen-style Personal Networking Gadget Package), which is nothing but the new discovery which is under developing stage by NEC Corporation. In this device you will find Bluetooth as the main

interconnecting device between different peripherals. P-ISM is a gadget package including five functions: a pen-style cellular phone with a handwriting data input function, virtual keyboard, a very small projector, camera scanner. P-ISMs are connected with one another through short-range wireless technology (Bluetooth). The whole set is also connected to the Internet through the cellular phone function. This personal gadget in a minimalist pen style enables the ultimate ubiquitous computing. HOW DOES IT WORK? The P-ISM(Pen-style Personal Networking Gadget Package) consists of a package of 5 pens that all have unique functions, combining together to create virtual computing experience by producing both monitor and keyboard on any flat surfaces from where you can carry out functions that you would normally do on your desktop computer. P-ISM's are connected with one another via a short-range (Bluetooth) wireless technology. The whole set is connected to the Internet through the cellular phone function.

The five components of P-ISM:

1. CPU PEN

   The functionality of CPU is done by one of the pens. It is also called computing engine

2. COMMUNICATON PEN

   Cell phone, pressure sensitive, pointer and earpiece, pointing device

3. VIRTUAL KEYBOARD

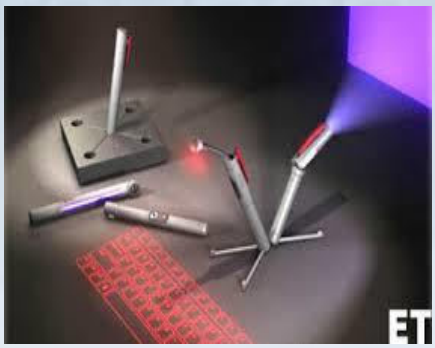
   Emits laser on to the desk where it looks like the keyboard having QWERTY arrangement of keys

4. LED PROJECTOR

   The role of monitor is taken by LED Projector which projects on the screen.

5. DIGITAL CAMERA

   It is useful in video recording, video conferencing, simply it is called as web cam

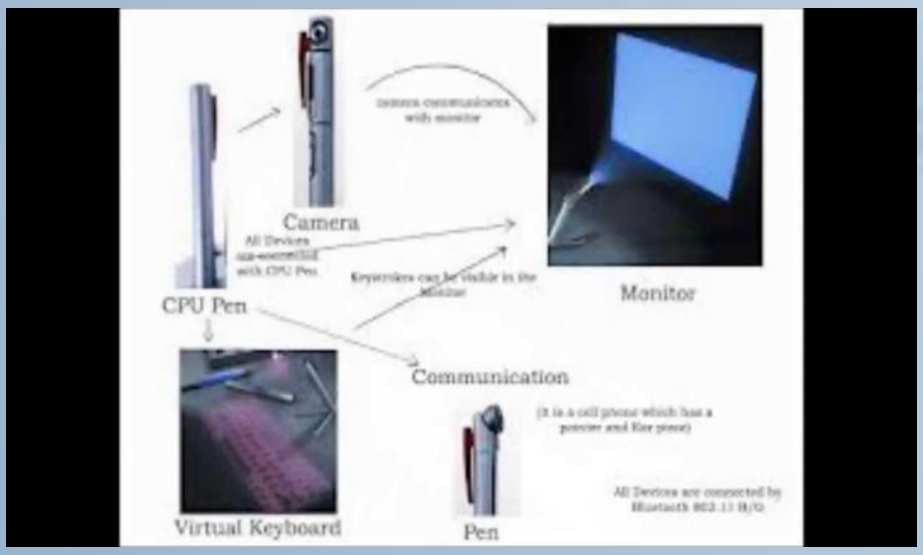


Battery

The most important part in the portable type of computer is its battery. Usually batteries must be small in size and work for longer time. It comes with a battery life of 6+. For normal use it can be used for 2 weeks.

Conclusion

The communication devices are becoming smaller and compact. This is only an example for the start of this new technology. We can expect more such developments



Anupama NC
I Year MCA

GOOGLE CLOUD GETS 'SNAPPY' WITH UBUNTU CORE SUPPORT

Ubuntu makes its way to Google Cloud with Docker support

Google has adopted for use in its cloud a streamlined version of the Canonical Ubuntu Linux distribution tweaked to run Docker and other containers. Ubuntu Core was designed to provide only the essential components for running Linux workloads in the cloud. An early preview edition of it, which Canonical calls "Snappy," was released last week. The new edition jettisoned many of the libraries and programs usually found in general use Linux distributions that were unnecessary for cloud use.

Canonical's "snappy" new formulation of Ubuntu has gained the support of another major public cloud vendor, with Google making the lightweight Linux available for customers of its Compute Engine IaaS offering. Ubuntu Core is a stripped-down version of the OS designed specifically for large-scale cloud deployments running applications in Docker containers. Developed based on lessons learned from Canonical's efforts to get Ubuntu running on phones, its compressed boot image clocks in at around 100MB

Unusually, Microsoft was the first cloud vendor to get on board with the new effort, offering support for launching Ubuntu Core instances via its Azure command-line tools. With Tuesday's announcement, Google, too, joins the party. The idea of offering a no-frills Linux variant for Docker deployments isn't unique to Ubuntu. It arguably originated with CoreOS, and even Red Hat has since come up with a bare-bones version of its Enterprise Linux.
But Ubuntu has the advantage of already being extremely popular for public cloud deployments. According to Digital Ocean – which web survey outfit Net craft says is now the third-largest hosting provider in the world – more than two-thirds of all machine instances in its cloud are running Ubuntu.

What's more, while Ubuntu Core provides a smaller OS footprint for running those workloads, it also offers an additional advantage, in the form of a new software update

management system that Canonical is calling "snappy." Unlike traditional, package-based update systems, snappy updates are transactional. All data is backed up before an update is applied, and if the update fails for any reason, the system can be rolled back to its former state.

Snappy updates are also easier to manage than those in traditional Linux systems. Instead of applications being composed of multiple packages – even hundreds of packages – with various interdependencies, each snappy application is a single unit. "I bet the average system on the cloud ends up with about three packages installed, total!" Canonical maestro Mark Shuttle worth used in a blog post earlier this month. "That's much easier to manage and reason about at scale." Some of those packages will be frameworks that provide services to other applications that depend on them. And the first such framework that's available for Ubuntu Core is – surprise, surprise – Docker.

For now, however, the Ubuntu Core images should be considered either alpha or beta software – depending on which of Canonical's marketing materials you read – and will remain so throughout Ubuntu's current development cycle. But if you'd like to check it out on Google's cloud now, Canonical has some instructions available here. It also remains available on Azure and as a KVM virtual machine image for trying out locally.

Deepika
I Year MCA