# 'Bash' computer bug could hit millions (Update)

September 25 2014, by Rob Lever


The US government and technology experts warned of a vulnerability in "Unix-based operating systems" powered by Linux and Apple's Mac OS, which could allow widespread and serious attacks by hackers

The US government and technology experts warned Thursday of a vulnerability in some computer-operating systems, including Apple's Mac OS, which could allow widespread and serious attacks by hackers.

The flaw affects "Unix-based operating systems" powered by Linux and Apple's Mac OS, said the warning from the US Computer Emergency Readiness Team (CERT), part of the Department of Homeland Security.

CERT said that if hackers exploit this they could take control of a PC: "Exploitation of this vulnerability may allow a remote attacker to execute arbitrary code on an affected system."

The agency said a patch was available for the flaw, which is described by security researchers as "Bash" or "Shellshock."

Some said the security hole would be more damaging than the "Heartbleed" bug which affected millions of computers worldwide earlier this year.

## 'Bigger than Heartbleed'

"This is going to be much bigger than Heartbleed," said Rahul Kashyap, chief security architect at Bromium Labs, a California-based security firm.

Kashyap said the Bash bug could affect millions of devices, from Web servers to Macintosh computers to webcams and other devices which connect to the Internet using open-source operating systems based on Linux.

Because the software is so prevalent, "it means attackers can get into your house, your home routers," Kashyap told AFP.

"They could deface a lot of websites on the fly. A lot of damage can be done, and it's a very simple code."

Even though no exploit of the flaw was seen in the first hours since the

vulnerability was made public, Kashyap said he expected "a huge impact in the next few days."

Independent security consultant Graham Cluley agreed that if hackers create a worm that exploits the flaw, "it would, without question, make the Bash bug a more serious threat than the Heartbleed OpenSSL bug that impacted many systems earlier this year."

While Heartbleed allowed unauthorized parties to spy on computers, "the Shellshock Bash bug allows attackers to hijack computers, and use them for their own purposes," Cluley said in a blog post.

## 'Staggering' potential

Gavin Millard at the security firm Tenable also expressed concern on the extent of the flaw.

"The potential for attackers utilizing Shellshock is huge," he said.

"With millions of Unix and Linux servers being vulnerable and running web services that hackers can connect to, the attack surface is staggering," he wrote in a blog post.

Johannes Ullrich at the SANS Internet Storm Center said the patch for the flaw "is incomplete" and that people using affected systems "should try to implement additional measures" which could include beefed-up firewalls or other software changes.

Eugene Kaspersky, who heads the Kaspersky Lab security group, said in a tweet that the flaw is serious.

The Bash bug "is BAD, expect a lot of exploits and hacked websites to be disclosed in the coming weeks," he wrote.

Researcher Robert Graham of Errata Security said that unlike Heartbleed, this bug "has been around for a long, long time. That means there are lots of old devices on the network vulnerable to this bug."

The computer security firm Symantec said it "regards this vulnerability as critical, since Bash is widely used in Linux and Unix operating systems running on Internet-connected computers, such as Web servers."

Symantec added in a statement: "Businesses, in particular website owners, are most at risk from this bug and should be aware that its exploitation may allow access to their data and provide attackers with a foothold on their network."

The news comes months after a panic among some security experts over Heartbleed, a flaw in a commonly used online platform for encrypted communications.

Internet users were advised to change passwords to online accounts or services, but only after checking to make sure the Heartbleed flaw was fixed and new certificates of online identity installed.

In the case of Bash, Kashyap said that users of computers and other devices should look to patch their systems quickly when updates become available but also cautioned to "watch out for scams, which could be fake updates" to install malware.