Heartbleed could harm a variety of systems

April 11 2014, by Bree Fowler

It now appears that the "Heartbleed" security problem affects not just websites, but also the networking equipment that connects homes and businesses to the Internet.

A defect in the security technology used by many websites and equipment makers have put millions of passwords, credit card numbers and other personal information at risk. The extent of the damage caused by Heartbleed isn't known. The threat went undetected for more than two years, and it's difficult to tell if any attacks resulted from it because they don't leave behind distinct footprints.

But now that the threat is public, there's a good chance hackers will try to exploit it before fixes are in place, says Mike Weber, vice president of the information-technology audit and compliance firm Coalfire.

Two of the biggest makers of networking equipment, Cisco and Juniper, have acknowledged that some of their products contain the bug, but experts warn that the problem may extend to other companies as well as a range of Internet-connected devices such as Blu-ray players.

"I think this is very concerning for many people," says Darren Hayes, professor of security and computer forensics at Pace University. "It's going to keep security professionals very busy over the coming weeks and months. Customers need to make sure they're getting the answers they need."

Here's a look at what consumers and businesses should know about

Heartbleed and its effects on networking devices.

— How is networking equipment affected?

Just like websites, the software used to run some networking equipment—such as routers, switches and firewalls—also uses the variant of SSL/TLS known as OpenSSL. OpenSSL is the set of tools that has the Heartbleed vulnerability.

As with a website, hackers could potentially use the bug as a way to breach a system and gather and steal passwords and other sensitive information.

— What can you do?

Security experts continue to advise people and businesses to change their passwords, but that won't be enough unless the company that created the software in question has put the needed fixes in place.

When it comes to devices, this could take a while. Although websites can be fixed relatively quickly by installing a software update, device makers will have to check each product to see if it needs to be fixed.

Both Cisco Systems Inc. and Juniper Networks Inc. continue to advise customers through their websites on which product is still vulnerable, fixed and unaffected. Owners may need to install software updates for products that are "fixed."

Hayes praises Cisco and Juniper for being upfront with customers. He cautions, though, that many other companies make similar products that likely have the bug, too, but haven't come forward to say so.

As a result, businesses and consumers need to check the websites for

devices that they think could have problems. They must be diligent about installing any software updates they receive.

Weber says that while there are some checks companies can do to see if their networking equipment is safe, they're largely beholden to the device makers to let them know what's going on.

Companies also need to make sure that business partners with access to their systems aren't compromised as well.

— Are other devices at risk?

Hayes says the bug could potentially affect any home device that's connected to the Internet, including something as simple as a Wi-Fi-enabled Blu-ray player.

He also points to recent advances in home automation, such as smart thermostats, security and lighting systems.

"We simply don't know the extent of this and it could affect those kinds of devices in the home," he says.