New Software Security Hole May Put Your Business at Risk

The federal government is warning that a newly discovered computer software vulnerability poses a major threat to the security of computer networks around the country.

Cyber criminals are exploiting holes in open-source code software commonly used in computer applications, websites and cloud services, which can allow them to seize control of a business's computer network if preventative measures are not taken.

This is not a threat that businesses should take lightly as it could cripple your organization if your network is affected. If your firm is large enough to have dedicated IT staff, it should be their focus now.

The danger

The vulnerability lies in the Log4j software library, written in the Java programming language and created by the Apache Software Foundation, a community of developers who write open-source software products that are free for organizations to use and are constantly being modified by the community.

Many software vendors incorporate the Log4j software library into products such as websites, applications and application services to record network security and performance information.

It is likely that some of the software that your business uses every day is built around Log4j. It runs on everything from cloud services to business enterprise software to internet-connected devices such as security cameras.

The federal Department of Homeland Security, the National Security Agency and other agencies announced on December 10 that they were "responding to active, widespread exploitation" of the vulnerability.

It warned that, if a company's software has this vulnerability, a criminal could take over the network and cripple the business.

What you should do

Do not take this threat lightly. As stated above, if you have dedicated IT staff, make it their primary focus right now.

Most importantly, you should hold a meeting with your staff to impart the importance of not clicking on links in suspicious e-mails. Hackers can break into a network only if they can deliver a line of malicious code to the Log4j library.

They do that by sending phishing e-mails and hoping recipients will open them.

Major software developers have reported that their products have the vulnerability, including:

- Microsoft
- McAffee
- Hewlett Packard
- IBM
- Dell
- Cisco
- Adobe
- Salesforce
- Oracle

You can find the full list of affected vendors and software here.

Apache has published three software patches to address the problem since it became known. Software developers who use Log4j are likely applying the patches and making updates to their software available to business users.

If you receive notification about an updated version of software you are using, it should be installed promptly.

Companies that do not have their own IT department, should contact computer network consultants as soon as possible to get advice on how to proceed.

The Cybersecurity & Infrastructure Security Agency has technical information on this threat on a dedicated website. IT experts should review the site's content, take appropriate actions as soon as possible, and monitor the site for further updates to the situation.

In the meantime, system administrators should adjust logging system settings so it does not interpret data as computer code. Antivirus software, using a virtual private network for remote access to the system, and being alert for phishing emails are also important protections. Sound network data security coupled with safe internet practices can protect your business's systems and your ability to continue operating.

###