U.S. warns on Java software as security concerns escalate

Jim Finkle, Rueters

The U.S. Department of Homeland Security urged computer users to disable Oracle Corp's Java software, amplifying security experts' prior warnings to hundreds of millions of consumers and businesses that use it to surf the Web.

Hackers have figured out how to exploit Java to install malicious software enabling them to commit crimes ranging from identity theft to making an infected computer part of an ad-hoc network of computers that can be used to attack websites.

"We are currently unaware of a practical solution to this problem," the Department of Homeland Security's Computer Emergency Readiness Team said in a posting on its website late on Thursday.

"This and previous Java vulnerabilities have been widely targeted by attackers, and new Java vulnerabilities are likely to be discovered," the agency said. "To defend against this and future Java vulnerabilities, disable Java in Web browsers."

Oracle declined to comment on the warning on Friday.

Java is a computer language that enables programmers to write software utilizing just one set of code that will run on virtually any type of computer, including ones that use Microsoft Corp's Windows, Apple Inc's OS X and Linux, an operating system widely employed by corporations.

Computer users access Java programs through modules, or plug-ins, that run Java software on top of browsers such as Internet Explorer and Firefox.

The U.S. government's warning on Java came after security experts warned earlier on Thursday of the newly discovered flaw.

It is relatively rare for government agencies to advise computer users to completely disable software due to a security bug, particularly in the case of widely used programs such as Java. They typically recommend taking steps to mitigate the risk of attack while manufacturers prepare an update, or hold off on publicizing the problem until an update is prepared.

In September, the German government advised the public to temporarily stop using Microsoft's Internet Explorer browser to give it time to patch a security vulnerability that opened it to attacks.

The Department of Homeland Security said attackers could trick targets into visiting malicious websites that would infect their PCs with software capable of exploiting the bug in Java.

It said an attacker could also infect a legitimate website by uploading malicious software that would infect machines of computer users who trust that site because they have previously visited it without experiencing any problems.

They said developers of several popular tools, known as exploit kits, which criminal hackers use to attack PCs, have added software that allows hackers to exploit the newly discovered bug in Java to attack computers.

Security experts have been scrutinizing the safety of Java since a similar security scare in August, which prompted some of them to advise using the software only on an as-needed basis.

At the time they advised businesses to only allow their workers to use Java browser plug-ins when prompted for permission by trusted programs such as GoToMeeting, a Web-based collaboration tool from Citrix Systems Inc.

Adam Gowdiak, a researcher with Polish security firm Security Explorations, subsequently said he had found other security bugs in Java that continued to make computers vulnerable to attack.

Java suffered another setback in October when Apple began removing old versions of the software from Internet browsers of Mac computers when its customers installed new versions of its OS X operating system. Apple did not provide a reason for the change and both companies declined comment at the time.

(Editing by Scott Malone, Steve Orlofsky and Bernadette Baum)

Source URL (retrieved on *07/30/2014 - 7:20pm*):
http://www.ecnmag.com/news/2013/01/us-warns-java-software-security-concerns-escalate?qt-video_of_the_day=0