Oracle says Java is fixed; feds maintain warning

January 14 2013, by Ryan Nakashima

The Oracle logo is displayed at Oracle headquarters on March 20, 2012. Oracle on Monday was distributing a patch for Java software flaws deemed so dangerous that the US Department of Homeland Security said that people should stop using it.

Oracle Corp. said Monday it has released a fix for the flaw in its Java software that raised an alarm from the U.S. Department of Homeland Security last week. Even after the patch was issued, the federal agency continued to recommend that users disable Java in their Web browsers.

"This and previous Java vulnerabilities have been widely targeted by attackers, and new Java vulnerabilities are likely to be discovered," DHS said Monday in an updated alert published on the website of its Computer Emergency Readiness Team. "To defend against this and future Java vulnerabilities, consider disabling Java in Web browsers until adequate updates are available."

The alert follows on the department's warning late Thursday. Java allows programs to run within websites and powers some advertising networks. Users who disable Java may not be able to see portions of websites that display real-time data such as stock prices, graphical menus, weather updates and ads.

Vulnerability in the latest version, Java 7, was "being actively exploited," the department said.

Java 7 was released in 2011. Oracle said installing its "Update 11" will fix the problem.

Security experts said that special code to take advantage of the weakness is being sold on the black market through so-called "Web exploit packs" to Internet abusers who can use it to steal credit card data, personal information or cause other harm.

The packs, sold for upwards of $1,500 apiece, make complex hacker codes available to relative amateurs. This particular flaw even enables hackers to compromise legitimate websites by taking over ad networks. The result: users are redirected to malicious sites where damaging software can be loaded onto their computers.

The sale of the packs means malware exploiting the security gap is "going to be spread across the Internet very quickly," said Liam O'Murchu, a researcher with Symantec Corp. "If you have the

opportunity to turn it off, you should."

Oracle said it released two patches—to address the flaw highlighted by the government, as well as another flaw that the government said was "different but equally severe."

As well, the patches set Java's default security level to "high" so that users will automatically be shown a prompt and given a chance to decline malicious software before it loads onto their computers.

Disabling Java completely in browsers has a similar effect, however. When websites appear without crucial functions, users can click a button to turn Java back on.

Making users aware when Java programs are about to be installed gives users a 50/50 chance of avoiding malware, said Kurt Baumgartner, a senior security researcher with Kaspersky Lab.

Many programmers are avoiding Java altogether, and its use in Web browsers is on the decline, he said.

Kaspersky Lab estimated that last year 50 percent of all website exploitations were due to vulnerabilities in Java. Adobe's Acrobat Reader accounted for another 28 percent of vulnerabilities.