

Fixes Released for Massive Internet Security Issue

On July 8th, technology vendors from across the industry will simultaneously release patches for their products to close a major vulnerability in the underpinnings of the Internet. While most home users will be automatically updated, it's important for all businesses to immediately update their networks. This is the largest synchronized security update in the history of the Internet, and is the result of hard work and dedication across dozens of organizations.

Earlier this year, professional security research Dan Kaminsky discovered a major issue in how Internet addresses are managed (Domain Name System, or DNS). This issue was in the design of DNS and not limited to any single product. DNS is used by every computer on the Internet to know where to find other computers. Using this issue, an attacker could easily take over portions of the Internet and redirect users to arbitrary, and malicious, locations. For example, an attacker could target an Internet Service Provider (ISP), replacing the entire web -- all search engines, social networks, banks, and other sites -- with their own malicious content. Against corporate environments, an attacker could disrupt or monitor operations by rerouting network traffic, capturing emails and other sensitive business data.

Mr. Kaminsky immediately reported the issue to major authorities, including the United States Computer Emergency Response Team (part of the Department of Homeland Security), and began working on a coordinated fix. Engineers from major technology vendors around the world converged on the Microsoft campus in March to coordinate their response. All of the vendors began repairing their products and agreed that a synchronized release, on a single day, would minimize the risk that malicious individuals could figure out the vulnerability before all vendors were able to offer secure versions of their products. The vulnerability is a complex issue, and there is no evidence to suggest that anyone with malicious intent knows how it works.

The good news is that due to the nature of this problem, it is extremely difficult to determine the vulnerability merely by analyzing the patches; a common technique malicious individuals use to figure out security weaknesses. Unfortunately, due to the scope of this update it's highly likely that the vulnerability will become public within weeks of the coordinated release. As such, all individuals and organizations should apply the patches offered by their vendors as rapidly as possible.

Since not every system can be patched automatically, and to provide security vendors and other organizations with the knowledge they need to detect and prevent attacks on systems that haven't been updated, Mr. Kaminsky will publish the details of the vulnerability at a security conference on August 6th. It is expected by this point the details of the vulnerability will be independently discovered, potentially by malicious individuals, and it's important to make the specific details public for our collective defense. We hope that by delaying full disclosure, organizations will have time to protect their most important systems, including testing and change management for the updates. Mr. Kaminsky has also developed a tool to help people determine if they are at

risk from "upstream" name servers, such as their Internet Service Provider, and will be making this publicly available.

Home users with their systems set to automatically update will be protected without any additional action. Vendor patches for software implementing DNS are being issued from major software manufacturers, but some extremely out of date systems may need to be updated to current versions before the patches are applied. Executives need to work with their information technology teams to ensure the problem is promptly addressed.

There is absolutely no reason to panic; there is no evidence of current malicious activity using this flaw, but it is important everyone follow their vendor's guidelines to protect themselves and their organizations.