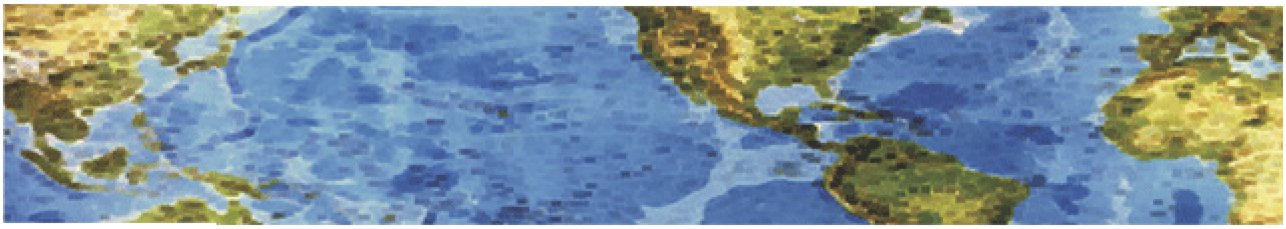
HALL ASSOCIATES



Risk-Based Decision Making Commentary
28 April 2014 Newsletter

DHS Says Stop Using Internet Explorer - Use of Other Browsers Recommended Until Situation Remediated

The Department of Homeland Security's U.S. Computer Emergency Response Team is urging online users to avoid using Internet Explorer, versions 6 through 11, in light of a vulnerability that exposes the Web browser to a zero-day exploit involved in recent targeted attacks. DHS urges users and administrators to "consider employing an alternative Web browser until an official update is available.“

http://www.govinfosecurity.com/

Microsoft warns of serious Internet Explorer flaw, but fix won’t cover XP users

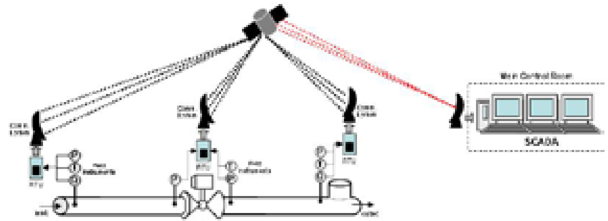
If you’re still using Windows XP, you do realize that Microsoft stopped supporting the operating system earlier this month, right? Now Microsoft has just said it’s been alerted to a serious security flaw in versions 6 through 11 of its Internet Explorer Web browser. The good news is it’s promising to roll out a fix for users soon; but the bad news is if you’re still using XP, you’ll get no fix, leaving your machine vulnerable to attack. **And other machines – check out the second article in this newsletter.**

According to Microsoft, the discovered flaw could allow a hacker to “gain the same user rights as the current user.” So they could potentially access your computer and operate it remotely. On a dedicated webpage giving more information about the flaw, the company explained: “An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

The Redmond-based company added, “On completion of this investigation, Microsoft will take the appropriate action to protect our customers, which may include providing a solution through our monthly security update release process, or an out-of-cycle security update, depending on customer needs.” But just to be clear, **this won’t cover XP users,** so if you’re still using the aging OS – and it’s estimated that around 20 percent of PCs continue to run it – you really should think about ditching it once and for all to shore up the security of your machine. In fact, the computer company told Reuters Sunday that Windows XP users should upgrade to one of two most recent versions of its operating system – Windows 7 or 8 – without delay.

Security firm FireEye claims to have uncovered the vulnerability, stating that most of the recorded attacks are targeting Internet Explorer versions 9 through 11.

http://www.foxnews.com/tech/2014/04/28/microsoft-warns-serious-internet-explorer-flaw-but-fix-wont-cover-xp-users/?intcmp=obnetwork



Windows XP Is Alive And Well in ICS/SCADA Networks

End-of-life for XP support not raising many red flags in critical infrastructure environments, where patching is the exception. Microsoft may have officially retired its Windows XP operating system this week, but that doesn't mean power plants and other critical infrastructure networks are dropping the now-unpatchable OS.

While there is no official public data on the number of XP systems running in ICS/SCADA environments, experts in that area say it's well represented, as are even older versions of Windows. Running insecure OSs may seem counterintuitive in such sensitive environments as power, gas, and oil industry networks, but it's a matter of priority: Patching remains rare in these networks for practical reasons, experts say. The no-patch mentality is a cultural one for the ICS/SCADA world that goes beyond Windows XP: **Safety and uninterrupted operations trump cyber security in those environments, and many of these systems never get the latest software updates for that reason.**

Overall, somewhere between 10 to 20 percent of organizations today actually install patches that their SCADA vendors are releasing, according to SCADA security experts. Utilities and ICS organizations face risks of power shutdowns if a newly patched system goes awry. Patching workstations and servers is less dicey than a factory-floor or power-generation system, and those systems are more likely to get patched than plant-floor systems, because they have shorter life spans and less direct impact on operations. Billy Rios, director of threat intelligence at Qualys, who has tested various ICS/SCADA and other embedded devices for security flaws, says the HMI (human-machine interface) and other applications atop XP in these process environments are more vulnerable than XP. "They really don't patch, anyway," Rios says. "And even if they did update, it's the software that's on top that's most vulnerable. The HMI software to run power plants and oil refineries is so riddled with bugs... it doesn't matter what OS it's running."

Many of these plant networks have controllers and other devices running Windows XP Embedded, a stripped-down version of the OS for specialized devices, which was not cut off by Microsoft this week as the full XP OS was, Rios notes. When you have a backdoor password in the HMI, it doesn't matter what OS you run. Someone can log in, regardless. You could upgrade to Windows 8 and still have problems.“ Dale Peterson, CEO of Digital Bond, an ICS/SCADA consultancy, says "There's a high correlation when we go into a site and start scanning and see they have XP systems. We see very little patching going on, and they may or may not have patched since they installed it," he says. "Those people can't be up in arms about Microsoft not supporting XP [anymore]. They'd rather not deal with the issue."

In a recent blog post, Peterson said: It doesn't matter if security patches exist or not if you are not going to apply them even as infrequently as annually. The fact that Microsoft is not issuing patches doesn't change their security posture one bit. In fact, some secretly are happy about this because they now have an excuse why they can't patch.

That doesn't mean all ICS/SCADA operators don't care about patching. The more security-aware ones are finding ways to update software where they can, and to ensure the update doesn't break their applications. "You can't do an upgrade of an OS without testing that your key applications that are supported by it. It's really basic IT practices that they need to adopt. I'm really glad XP [end-of-life] happened. It made a lot of people who care about this think through those issues."

Paul Asadoorian, product evangelist for Tenable Network Security, says while the threat to these XP systems indeed is there, power plant operators prefer to add more monitoring or other defenses to watch for malware and attacks than to change out software. "[Much] of this industry has put in appropriate protections," Asadoorian says. "They are hesitant to [patch] because these devices are controlling valves in nuclear plants and water plants." So, instead, they tend to monitor for malware, and, increasingly, some are looking at whitelisting technology as well as specialized firewalls and gateways. ***(My Opinion – these are NOT appropriate protections to the malware and cyber disruption capabilities that are continually being upgraded. Both monitoring and whitelisting have been shown to be inadequate.)***

Asadoorian says he once pointed out malware to an ICS workstation, and the operator shrugged it off. "'I push this button and the valve opens either way," the plant operator told Asadoorian. Says Rios of the exchange: "It was very clear that the priority was for the system to operate even if it has malware." These plants tend to focus more on physical security and firewalls or unidirectional gateways to cordon off critical systems. "The truth is they have soft interiors," says Andrew Ginter, vice president of industrial security at Waterfall Security. "And every change is a threat to safety and reliability... So change is very slow, and that's why see still see XP hanging around. It's trusted and understood."

Ginter says most XP implementations are in PLCs, RTUs, and concentrators. "It might be true of XP that the vendor has stripped it down so it's smaller and easier to manage. That's not the same as desktop XP," he says. "But it's still XP and still under the same vulnerabilities."
http://www.darkreading.com/informationweek-home/windows-xp-alive-and-well-in-ics-scada-networks/d/d-id/1204385

There are any number of scary predictions, Google for hundreds. Here are a few to start with:
Inside the Ring: U.S. power grid defenseless from physical and cyber attacks
http://www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defenseless-from-att/

Protecting Our Nation's Critical Infrastructure from Cyber Threats http://www.dhs.gov/protecting-our-nations-critical-infrastructure-cyber-threats

International Journal of Critical Infrastructure Protection
http://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection/