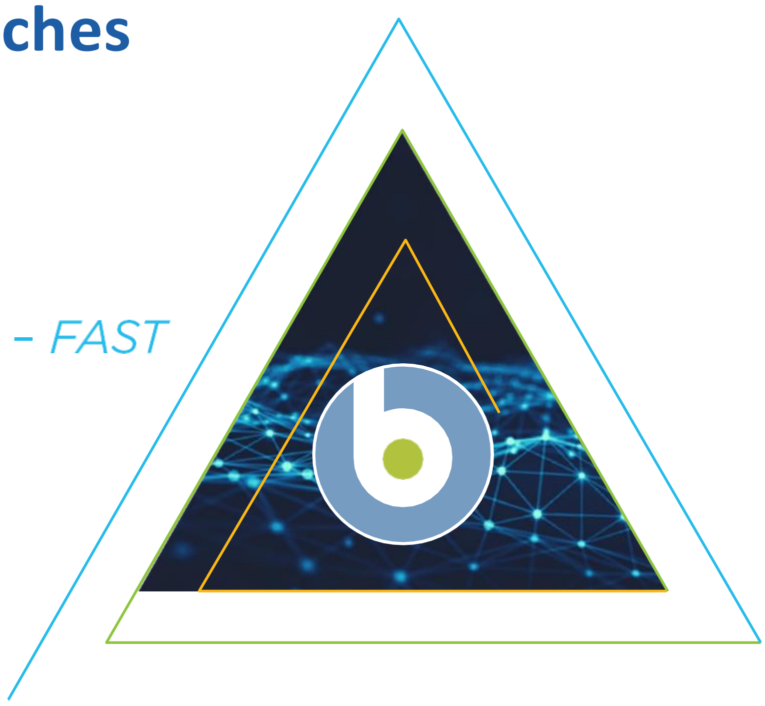
HCL SOFTWARE | BIGFIX

Continuous Wave of Critical Windows Patches Emphasizes Need for Speed and Automation

Find and Fix All Endpoints



Overview

The recent wave of critical Windows vulnerabilities emphasizes the need for fast and effective patching. Most attackers exploit known vulnerabilities and implementing patch best practices is key to protecting your endpoints and your organization from cyberattacks.

On August 13th, 2019, Microsoft released a couple of patches for Remote Desktop Services to address two critical vulnerabilities: CVE-2019-1181 and CVE-2019-1182. According to the National Vulnerability Database, these CVEs carry an impact severity of 9.8 (using the CVSS v3.0 Severity calculator). In other words, these patches are critically important since malware could exploit these vulnerabilities and propagate between vulnerable computers without user interaction. These patches should be applied to Windows 7 SP1, Windows Server 2008 R2 SP1, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, and all supported versions of Windows 10. At the same time, Microsoft delivered another patch, CVE-2019-1162, for Windows 10 after Google's Project Zero identified a vulnerability which has existed within Windows for 20 years, beginning with Windows XP. According to Microsoft, an attacker who successfully exploits this vulnerability could run arbitrary code in the security context of the local system; then install programs; view, change, or delete data; or create new accounts with full user rights.

System Administrators are urged to expedite testing and deployment of these Windows patches. Microsoft accumulates security patches over a month and dispatches them all on the second Tuesday of each month. Every time they do, administrators must evaluate, test and install those patches across their Windows environment. Speed is very important since endpoints are most vulnerable to attack

Patch with Speed and Accuracy

Patch automation can significantly reduce the patch time while increasing first pass success rates. Here are a couple of ideas: First, consider using BigFix Autopatch. This feature gives you the ability to create rules for distributing patches to your organization in an automated fashion. Second, BigFix users should consider using Autopatch and setting a schedule to distribute patches automatically to groups of client devices according to prescribed maintenance windows. A recommended best practice is to deploy patches to three groups of client devices as described below.

Group	Percentage of Devices	Description	Execution Date
1. Pilot Client Devices	1%	Pilot group as defined by administrators.	Patch Tuesday + 1 day
2. IT and First Adopters	9%	Group defined by IT team members and sometimes a random sampling of devices.	Staggered from (Patch Tuesday + 2 days) to (Patch Tuesday + 5 days)
3. Remaining Client Devices	90%	All remaining client devices not in the first or second groups.	Staggered from (Patch Tuesday + 6 days) to (Patch Tuesday + 10 days)

If a patch causes a problem after the first or second group deployments, administrators should exclude that patch from the next deployment(s). Additionally, the flexibility of BigFix will facilitate adapting this best practice to your organization's policies and implementing what makes sense to your business.

For more information

Visit **www.BigFix.com** and schedule a demo or download trial software. Also visit **support.BigFix.com** to watch the recorded webinar, *August Microsoft Patch Content Review,* originally held on August 14, 2019.

About HCL Software

HCL Software is a division of HCL Technologies (HCL) that operates its primary software business. It develops, markets, sells, and supports over 20 product families in the areas of DevOps, Automation, Digital Solutions, Data Management, and Mainframes. HCL Software has offices and labs around the world to serve thousands of customers. Its mission is to drive ultimate customer success with their IT investments through relentless innovation of its products.

Learn more: **https://www.hcltechsw.com**