SENT 07-15-2021.
ATTACHMENTS: 0

SANDBOX TECHNOLOGIES

Urgent Notification

Microsoft Security Vulnerability “PrintNightmare”

Recently, a series of exploits were discovered that can potentially impact organizations using the almost ubiquitous Microsoft Print Spooler service.

The exploits allow malicious actors to effect what are known as “local privilege escalation” and “remote code execution” on affected networks. The matter has been assigned a CVSS score of 8.8, which is considerable in terms of severity.

When first announced, a patch had not been released to the public. In keeping with best practices, we followed CISA’s recommendation and began proactively disabling print spoolers on Windows Domain Controllers as a temporary means of mitigating exposure. Soon after, Microsoft released a patch to remediate the issue, however it was almost immediately found to be ineffective.

Microsoft has now released a second patch to resolve the issue. Initial testing has found the patch to be effective, and as such we are undertaking the process of deploying it to our client networks.

The application of this patch requires both re-boots, and in some cases, manual registry inspections. Recognizing that many of our clients may be ill-positioned to sustain downtime during business hours, we are scheduling application of the fixes to occur outside of normal business hours.

Notwithstanding the foregoing, we also recognize that some clients may wish to have this remediation made immediately. **Whether you would like us to do so out of an abundance of caution, to avoid incurring the added cost of after-hours labor, to avoid interrupting business-critical activities outside of normal hours, or all of the above, we will be happy to accommodate you. Simply respond to this email or inform your engineer or CCIO that you would like to make alternative arrangements.**

If we do not hear from you, the aforementioned patch application will be performed sometime between the hours of 6:00 P.M. and 7:00 A.M. in the coming days. As always, we will attempt to minimize the cost to our clients through the use of automation (when possible). To the extent staffing and time permit, we will also endeavor to begin downloading patches and inspecting registries during normal business hours, leaving the disruptive components of this effort for after hours.

For those interested in learning information about PrintNightmare, we have found the following article from our colleagues at Sentinel One.

https://www.sentinelone.com/blog/printnightmare-latest-patch-almost-puts-microsoft-vulnerability-to-bed/

As always, if you have any questions regarding this matter, please feel free to reply to this email, contact our remote support helpdesk, or consult your Sandbox Technologies Engineer or CCIO.

Chris Harper
Chief Security Officer
Sandbox Technologies, Inc

Our mailing address is:
4111 West Alameda Ave., Suite 605 Burbank, CA 91505