O'Melveny

Alerts & Publications

Failure to Apply Recent Microsoft Patch May Create Legal Liabilities

January 15, 2020

KEY CONTACTS

Lisa Monaco
Washington, DC
D: +1-202-383-5413

John Dermody
Washington, DC
D: +1-202-383-5306

On Tuesday, January 14, Microsoft released a patch to close an important vulnerability related to security certificate functions in Windows 10, Windows Server 2016, and Windows Server 2019. Windows users should ensure that their systems have been updated to mitigate cyber risk and avoid possible legal exposure.

The patch is particularly noteworthy because it addresses a vulnerability that would allow malware to masquerade as legitimate, digitally signed software. This would permit malicious cyber actors to bypass existing security measures and gain access to internal networks and data. The National Security Agency discovered the vulnerability and disclosed it to Microsoft, likely after going through the Vulnerabilities Equities Process, the internal process by which the government determines whether and when to disclose vulnerabilities it discovers. The vulnerability is significant enough that Anne Neuberger, the head of the National Security Agency's Cybersecurity Directorate, publically commented on the matter.

As we have seen in the fallout from the WannaCry and NotPetya attacks, failing to quickly patch vulnerabilities can leave systems exposed to ransomware attacks and data breaches. This risk is heightened after the announcement of a major patch as hackers may turn their focus to developing new exploits based upon the announcement or may seek to deploy an existing exploit before systems are patched.

Failure to timely patch computer systems can lead to cyber incidents and related legal liability. Equifax's failure to timely patch its network was a critical factor in the US$575 million global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and state attorneys general. Federal regulators and state enforcement officials, particularly for those states requiring implementation of "reasonable security" for computer networks, consider patching to be a baseline requirement of any cybersecurity program. Indeed, the California Attorney General noted in the 2016 California Data Breach report that "[k]eeping up-to-date in patching newly discovered vulnerabilities is critical." Finally, the failure to implement baseline security measures like vulnerability patching could invalidate cyber insurance coverage, depending upon the terms of the policy.

In the wake of Microsoft's announcement, and as a general practice, in-house counsel should be coordinating with relevant IT personnel to ensure that security practices are up to date.

This memorandum is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Steve Bunnell, an O'Melveny partner licensed to practice law in the District of Columbia, Lisa Monaco, an O'Melveny partner licensed to practice law in New York, and John Dermody, an O'Melveny counsel licensed to practice law in California, contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.