BISHOP FOX

8240 S. Kyrene Road
Suite A-113
Tempe, AZ 85284

P 480 621 8967
F 480 383 6401
www.bishopfox.com

CVE-2017-11779 FAQS

Can you describe the vulnerabilities patched by Microsoft today? **Microsoft has patched three issues related to how Windows processes certain DNS messages. These messages usually include information that your computer needs to access a domain name (like typing http://www.google.com in your browser, or Outlook checking for new email). Some versions of Windows don't thoroughly check the format of these messages, which could allow a remote attacker to gain control of your computer.**

What are the affected products? **Windows 8 through Windows 10, and Windows Server 2012 through 2016.**

How can this vulnerability be triggered? **The attacker needs to respond to DNS queries that your computer makes. This is only possible if they are on the same network as you (e.g., shared Wi-Fi at an airport).**

Walk me through a theoretical attack. Does it rely on the user being online? **A user doesn’t need internet access for this attack to work, but they must be connected to a network. One plausible way would be via a man-in-the-middle attack targeting shared Wi-Fi. For example, if you join your local coffee shop Wi-Fi and someone on the network messes with traffic so that all network communications made by your laptop would be directed to the attacker’s computer. Then when your laptop made a DNS request (which happens regularly, even without the user doing anything), the attacker could respond with malicious data that would trigger this vulnerability. Successful exploitation would enable the attacker to execute code on your computer, and gain control of your files and accounts.**

What does this mean for the average user? What does it mean for the average business? **The average user’s biggest concern would be the scenario that their laptop (corporate or otherwise) is exposed to a malicious Wi-Fi network, or if an attacker has access to a wired network they are connected to. If an attacker has a foothold in your corporate network, they may exploit this issue to gain access to additional systems, possibly stealing sensitive information about customers or operations.**

How do we protect ourselves from these vulnerabilities? **These are the types of vulnerabilities that attackers love because it gives them “the keys to the**

kingdom.” As such, both enterprise and consumer Windows users need to make it a priority to apply the patch provided by Microsoft in their October security update.

Are vulnerabilities like this common? **Broadly speaking, this type of vulnerability is fairly common. Though there haven’t been any public issues in Windows DNS code for some time, Microsoft (and Apple in addition to other major companies) regularly provide patches against this kind of issue in other components of their code.**

What can we learn from this? Why is this so important? **High-profile services and applications will always contain vulnerabilities that are merely waiting to be discovered. It’s important to have an incident response plan for the inevitable day that you are compromised. Then, you can focus on what matters, which is detecting and recovering from the compromise. Back up often, and to more than one location. It's still important to patch your systems as soon as you can after a patch is available, as once an issue is public, more parties are aware of the flaw and they can work to exploit unpatched systems.**

Are there anti-exploit mitigations in Windows that help address this exploit? **There are mitigations that make this issue harder to exploit, but they will not outright prevent an attacker from gaining access.**

Does this mean DNSSEC is a problem to worry about? **DNSSEC isn’t much of a concern for end users; its primary focus is between DNS servers, not between users and DNS servers.**

Do you have any indication that these vulnerabilities are already being exploited in the wild? **At this time, we have no indication that these vulnerabilities have been exploited.**