Cybersecurity Advisory for Patching	**Cyber Advisory**
Criticality:Yellow:Medium-High	**05/28/2019 12:30 PM**

Summary	Malicious actors are taking advantage of and actively scanning for devices that have not been patched for the EternalBlue and BlueKeep Microsoft vulnerabilities. As of today, almost 1 million Windows computers are vulnerable to BlueKeep. ***Because this vulnerability requires no user action, it could cause devastating harm to vulnerable computer systems.*** The ACTIC strongly recommends all organizations apply security patches for the EternalBlue (CVE-2017-0144) and BlueKeep (CVE-2019-0708) vulnerabilities.
Criticality	Criticality is ***medium-high***, based on current activity and potential for harm. Note: See below for criticality criteria.
About the Vulnerabilities	EternalBlue is an exploit developed by the National Security Agency and released publicly by the Shadow Brokers hacking group on April 14, 2017. EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. A remote attacker can send specially crafted packets to vulnerable computers to run programs (execute arbitrary code remotely). BlueKeep is a vulnerability in Microsoft's Remote Desktop Services – formerly known as Terminal Services. To exploit this vulnerability, an attacker needs to send a specially crafted request to the target system's Remote Desktop Service via remote desktop protocol (RDP). The attacker does not need an account on the target computer (the vulnerability is pre-authentication) and requires no user interaction. An attacker who successfully exploits this vulnerability could execute arbitrary code on the target system — install programs; view, change, or delete data; or create new accounts with full user rights.
Activity	The EternalBlue vulnerability may have been used to help spread WannaCry, NotPetya, and RobbinHood ransomware that recently devastated City of Baltimore. To clarify, many ransomware incidents start with a phishing email or compromised account credentials. Some media reports are stating attackers used this vulnerability to spread ransomware throughout the targeted organization making the attack more destructive. Over the Memorial Day weekend, a threat intelligence firm detected scans for Windows systems vulnerable to BlueKeep. It appears that at least one threat actor is investing significant time and effort into compiling a list of vulnerable devices, most likely in preparation for actual attacks.

Recommended Actions	Apply security patches for the EternalBlue (CVE-2017-0144) and BlueKeep (CVE-2019-0708) vulnerabilities. For EternalBlue, the only mitigation is to patch vulnerable computers. For BlueKeep, disabling Remote Desktop Services and blocking TCP port 3389 (RDP) at the enterprise perimeter firewall will help mitigate the vulnerability. Patches are available at • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144 • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
For More Info	Listed below are links to more information. • https://thehackernews.com/2019/05/bluekeep-rdp-vulnerability.html • https://en.m.wikipedia.org/wiki/EternalBlue • https://www.ehackingnews.com/2019/05/ransomware-tool-causing-chaos-in.html • https://blog.erratasec.com/2019/05/a-lesson-in-journalism-vs-cybersecurity.html
To Report Suspicious Activity	Please report potential, suspected, and/or confirmed cyber threats to the ACTIC. Provide known or suspected • Threat/attack method • Indicators of compromise • Adversary(ies) • Impact, and • Any other threat actor characteristics. Note: The ACTIC shares victims' applicable critical infrastructure sector and scale of operations (national, regional, state, or local level). ***The ACTIC does not share any identifying information without the victim's consent.*** Please report suspicious activity to the ACTIC via: • http://www.azactic.gov/Tips/ • ACTIC@AZDPS.GOV • (602)644-5805 or (877) 2 S A V E A Z (272- 8329)

Criticality Criteria	Listed below is a general description of the criticality rating. The rating is subjective based on information currently known and the analyst's experience. • High / Red: The potential incident may impact or breach critical business, systems, and/or services without immediate intervention. There may also be indications that an attack is currently in process. • Medium / Yellow: The potential incident does not place an organization's business, systems, and/or services in immediate risk but may pose an unacceptable risk if not addressed in a timely fashion. • Low / Green: The potential incident does not pose unacceptable risk but may indicate trends or patterns that might suggest a future impact. • Informational / White: There no current potential incident. Information is for awareness.
Disclaimer	This alert contains raw intelligence that has not been analyzed. It is provided for your situational awareness to help improve Arizona's cyber resiliency. While this document may mention vendors' products and services, the ACTIC does not recommend or endorse any specific ones.