## Unpatched Operating Systems

**Severity**: Informational Low Medium High Critical **CVSS Score**: {{CVSS-SCORE}}

**CVSS Calculation**: {{CVSS-CALC}}

**Likelihood** : High Medium Low({{LIKELIHOOD}}) **Impact** : High Medium Low ({{IMPACT}}) **Risk**: Very High High Medium Low Very Low ({{RISK-TOTAL}})

### Vulnerability Description

Keeping software and operating systems up to date ensures they have the most up to date security. New vulnerabilities are constantly being found and fixed. When patches are released it is becoming common for attackers to reverse engineer them and develop exploits. This means it can be critical to patch software quickly to reduce the risk of exploitation.

Some vulnerabilities become popular, with efficient and freely available tooling to exploit them. This can make it easy for even unskilled attackers to abuse unpatched software.

Different vulnerabilities hold different risks, from disclosing information an attacker could use, all the way to being able to remotely execute code on vulnerable computers.

### Vulnerability Detail

Tools to perform this exploit are freely available and the exploit itself is well known, so an attacker could easily find and exploit this vulnerability.

In this instance, the exploit allowed full access to the local computer.

The operating system has reached the end of line and so will no longer receive security updates.

### Remediation Advice

Ensure the operating system is updated with all of the currently available patches.

{{SPECIFIC-REMEDIATIONS}}

A patching policy should be in place to ensure that both operating systems and software are regularly updated to prevent known vulnerabilities impacting the security of the environment.

Further information:

* [Security Update for Microsoft Windows SMB Server](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010)
* [What is EternalBlue?](https://www.avast.com/c-eternalblue)
* [Metasploit - EternalBlue](https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/)
* [WannaCry Ransomware](WannaCrypt%20ransomware%20worm%20targets%20out-of-date%20systems)