CVE-2020-1147: .NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability

Executive Summary

On July 14, 2020, Microsoft released a patch for CVE-2020-1147. If left unpatched the vulnerability, which affects Microsoft SharePoint, .NET Framework, and Visual Studio, could allow an attacker to run arbitrary code. According to Microsoft, this type of vulnerability is historically exploited by attackers. To patch the vulnerability, the most recent software needs to be installed for the affected programs. This vulnerability should be carefully considered for patching by any healthcare organization with special consideration to the vulnerability criticality category against the risk management posture of the organization.

Analysis

According to Microsoft, "[The vulnerability exists] when the software fails to check the source markup of XML file input. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the process responsible for deserialization of the XML content."

To exploit this vulnerability, an attacker could upload a specially crafted document containing malicious code in the source markup in XML content to a server using an affected product to process content. Microsoft's exploitability assessment states that "Exploitation More Likely" for both the latest and older software releases. This assessment means that "that exploit code could be created in such a way that an attacker could consistently exploit this vulnerability" and that historically this type of vulnerability is exploited by attackers making it an "attractive target."

Alert

On July 14, 2020, Microsoft released 123 patches for known vulnerabilities. Among the Common Vulnerabilities and Exposures (CVE) patched is CVE-2020-1147, a remote code execution vulnerability affecting Microsoft SharePoint, .NET Framework, and Visual Studio.

Patches, Mitigations & Workarounds:

CVE-2020-1147 is patched when the following programs are updated to the most recent version of the software:

- .NET Core
- .NET Framework
- SharePoint Enterprise Server (2013 and 2016)
- SharePoint Server (2010 and 2019)
- Visual Studio (2017 and 2019)

References

https://www.helpnetsecurity.com/2020/07/21/cve-2020-1147/

https://www.helpnetsecurity.com/2020/07/14/july-2020-patch-tuesday/

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1147