CYBERSECURITY VULNERABILITIES OF INTEREST TO THE HEALTH SECTOR

In recent days, a number of vulnerabilities in common information systems which are relevant to organizations in the healthcare sector have been disclosed to the public. These vulnerabilities are from Microsoft and Adobe as well as highlights from a joint DHS/FBI report on the most impactful vulnerabilities in recent years. The vulnerabilities highlighted in this report have been selected because they meet two criteria. First, they are significant in that they have the potential to allow an attacker to cause significant harm to the target organization. Second, they are likely to be included in the enterprise infrastructure of a healthcare organization. Further details on these vulnerabilities can be found below, along with their potential effects if exploited as well as patches.

Please note: If you are only in possession of a hard copy of this alert, for your convenience, all hyperlinks contained in the text also appear in the references section.

Microsoft

On Tuesday, May 12, Microsoft announced 111 vulnerabilities including several high-priority bugs in some of their common applications as well as Windows. The full details of the Microsoft May 2020 release can be found here.

Microsoft released patches for four Remote Code Execution (RCE) vulnerabilities in SharePoint, one in their graphics component management system, an Elevation of Privilege vulnerability in their web browser, Edge, and three Memory Corruption vulnerabilities in their operating system, Windows:

Product	Vulnerability	CVE	Link to patch
Office SharePoint	Remote Code Execution	CVE-2020-1069	Patch
Office SharePoint	Remote Code Execution	CVE-2020-1102	Patch
Office SharePoint	Remote Code Execution	CVE-2020-1024	Patch
Office SharePoint	Remote Code Execution	CVE-2020-1023	Patch
Graphics Component	Remote Code Execution	CVE-2020-1153	Patch
Edge	Remote Code Execution	CVE-2020-1056	Patch
Windows	Memory Corruption	CVE-2020-1028	Patch
Windows	Memory Corruption	CVE-2020-1136	Patch
Windows	Memory Corruption	CVE-2020-1126	Patch

Remote code execution vulnerabilities are especially egregious as they not only allow at attacker to execute code on the target system but also to do so remotely, giving them effective total control of the system and a pivot point to further attack other systems on the enterprise network. Elevation of Privilege vulnerabilities allow an attacker who has compromised a low-level account to operate as if they have administrative access to the target system, increasing the opportunities to wreak havoc, Memory Corruption vulnerabilities allow for the improper handling of memory which have the potential to allow an attacker to install a program, modify or delete information or create an account with maximum privileges. All of these patches have a priority of critical and as such, should be patched immediately. An explanation of Microsoft's severity rating system can be found here.

Adobe

On Tuesday, May 12, Adobe announced 36 vulnerabilities including 16 that were classified as "critical". Several of these vulnerabilities can lead to arbitrary code execution or security feature bypass, both of which represent significant threats to healthcare infrastructure. The most egregious are below:

Product	Vulnerability	CVE(s)	Link to patch
Acrobat and Reader	Heap Overflow – Arbitrary Code Execution	CVE-2020-9612	Patch
Acrobat and Reader	Race Condition – Security feature bypass	CVE-2020-9615	Patch
Acrobat and Reader	Out-of-bounds write – Arbitrary Code Execution	CVE-2020-9597 CVE-2020-9594	Patch
Acrobat and Reader	Security feature bypass	CVE-2020-9614 CVE-2020-9613 CVE-2020-9596 CVE-2020-9592	Patch
Acrobat and Reader	Buffer error – Arbitrary Code Execution	CVE-2020-9605 CVE-2020-9604	Patch
Acrobat and Reader	Use-after-free – Arbitrary Code Execution	CVE-2020-9607 CVE-2020-9606	Patch

Arbitrary Code Execution vulnerabilities, similar to the Remote Code Execution vulnerabilities previously described, have the potential to allow at attacker to execute code on the target system giving them effective total control of it and possibly allowing it to become a pivot point to further attack. Security Feature Bypasses allow for attackers to circumvent security features designed in products. These vulnerabilities can be significant due to the fact that, once exploited, threat actors can maneuver and operate in ways that victims assume is not possible, due to the belief that the security features are fully functional. All of these patches have a priority of critical and as such, should be patched immediately. An explanation of Adobe's severity rating system can be found here.

DHS/FBI Joint Vulnerability Alert

On Tuesday, May 12, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a joint alert summarizing the top 10 most routinely exploited vulnerabilities, with a focus on those identified from 2016 to 2019. These were specifically vulnerabilities exploited by sophisticated foreign actors, implying Advanced Persistent Threats (APTs), but the report also covered vulnerabilities targeted by non-state and unattributed actors. According to the Alert, Microsoft's OLE (Object Linking and Embedding) was the most exploited technology (CVE-2017-11882, CVE-2017-0199, and CVE-2012-0158) with Apache Struts being the second most attacked technology. They also noted that with everyone shifting to remote work due to the Coronavirus that misconfigured Office 365 deployments are creating a large attack surface and they also noted continuing challenges such as poor employee training on social engineering and a lack of system recovery and contingency plans. HHS recommends the healthcare industry examine this bulletin carefully, with special emphasis on the specific vulnerabilities identified above.

References

- Microsoft Vulnerabilities released for May 2020
  https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-May

- CVE-2020-1069 | Microsoft SharePoint Server Remote Code Execution Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1069

- CVE-2020-1102 | Microsoft SharePoint Remote Code Execution Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1102

- CVE-2020-1024 | Microsoft SharePoint Remote Code Execution Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1024

- CVE-2020-1023 | Microsoft SharePoint Remote Code Execution Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1023

- CVE-2020-1056 | Microsoft Edge Elevation of Privilege Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1056

- CVE-2020-1153 | Microsoft Graphics Components Remote Code Execution Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1153

- CVE-2020-1028 | Media Foundation Memory Corruption Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1028

- CVE-2020-1136 | Media Foundation Memory Corruption Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1136

- CVE-2020-1126 | Media Foundation Memory Corruption Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1126

- Security Update available for Adobe Acrobat and Reader | APSB20-24 (May 2020)
  https://helpx.adobe.com/security/products/acrobat/apsb20-24.html

- Adobe Severity ratings
- https://helpx.adobe.com/security/severity-ratings.html

- Microsoft Security Update Severity Rating System
- https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system

- Microsoft May 2020 Security Updates
- https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-May

- CVE-2020-9612
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9612

- CVE-2020-9615
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9615

- CVE-2020-9597
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9597

- CVE-2020-9594
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9594

- CVE-2020-9614
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9614

- CVE-2020-9613
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9613

- CVE-2020-9596
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9596

- CVE-2020-9592
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9592

- CVE-2020-9605
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9605

- CVE-2020-9604
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9604

- CVE-2020-9607
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9607

- CVE-2020-9606
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9606

- Microsoft OLE Background
- https://docs.microsoft.com/en-us/cpp/mfc/ole-background?view=vs-2019

- CVE-2017-11882
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

- CVE-2017-0199
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

- CVE-2012-0158/MS12-027
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-027