CYBERSECURITY VULNERABILITIES OF INTEREST TO THE HEALTH SECTOR

In recent days, a significant number of vulnerabilities in common information systems relevant to the healthcare sector have been disclosed to the public. These vulnerabilities are from Microsoft, Adobe, Oracle, Cisco and Google, as well as others. These vulnerabilities should be carefully considered for patching by any healthcare organization with special consideration to each vulnerability criticality category against the risk management posture of the organization.

MICROSOFT

On Tuesday, July 14, Microsoft announced 123 vulnerabilities, the second largest number of Patch Tuesday fixes ever, including several high-priority bugs in the Windows operating system and several Office applications. The full details of the Microsoft July 2020 release can be found here, which included

The most severe vulnerability was discovered by Checkpoint and is called SigRed. It's a remote code execution (RCE) in Windows Domain Name Server (DNS), applicable to all versions of Server (2003 to 2019). This exploit is tracked as CVE-2020-1350, has a CVSS of 10 of 10 and can be exploited with self-propagating (wormable) malware. The vulnerability is specifically in how a Windows DNS server parses an incoming DNS query and how it forwards queries. It allows an attacker to craft a malicious DNS query. The vulnerability is a heap-based buffer overflow, and when triggered, because it's on a Widows server it can allow for Domain administrator Rights. In practical terms, the attacker can gain total control over the most important system in a Windows Domain environment - the server. The attacker could potentially intercept and modify emails or network traffic, disable services and collect user credentials. There are limited circumstances in which this attack can be launched remotely, through browser sessions.

Other significant vulnerabilities patched include RCEs in Windows HyperV hypervisor, the Jet Database Engine, multiple Office products including Word, Excel, Outlook and SharePoint as well as windows LNK shortcut files and several Windows graphic components. Cisco Talos released Snort rules for several of these vulnerabilities.

ADOBE

Adobe announced thirteen vulnerabilities that it patched on July's Patch Tuesday, four of which were classified as "critical". These affect five products: Download Manager, ColdFusion, Genuine Service, Media Encoder and the Creative Cloud Desktop Application. The four critical vulnerabilities:

- A command injection flaw is with the Download Manager for Windows. It contains a command injection flaw (CVE-2020-9688) which can lead to arbitrary code execution
- Two out-of-bounds write condition vulnerabilities in Media Encoder for Windows that can lead to arbitrary code execution (CVE-2020-9646 and CVE-2020-9650)

- The final critical vulnerability was an arbitrary file system write vulnerability in Creative Cloud Desktop (CVE-2020-9682)

ORACLE

Oracle announced 443 vulnerabilities that it patched for its quarterly patch cycle. Several of these have a CVSS score of 10 or 9.8 and hundreds of them are remotely exploitable. Below is a brief breakdown of the Oracle platforms most likely used by healthcare organizations and the corresponding vulnerabilities as part of this release:

Application	Patches	Remotely exploitable (without authentication)
Oracle Communications Applications	58	45
Oracle E-Business Suite	29	23
Oracle Enterprise Manager	14	10
Oracle Financial Services Applications	38	26
Oracle Fusion Middleware	53	49
Oracle MySQL	40	6
Oracle Retail Applications	39	34
Oracle Siebel CRM	5	5
Oracle Supply Chain	22	18
Oracle Database Server	20	1
Oracle GoldenGate	3	1

Table 1: A summary of the most likely Oracle vulnerabilities to affect healthcare information infrastructure

CISCO

In mid-July, Over the course of several days Cisco released 33 vulnerability patches including 6 categorized as critical as well as 11 categorized as high severity. The critical vulnerabilities affect VPN routers and firewalls and the Cisco Prime License Manager. The types of vulnerabilities include remote code execution, authentication bypass, privilege escalation and static default credential vulnerabilities.

GOOGLE

Google released Chrome version 84 with with new security updates this week. It is considered a significant release, especially regarding the fundamental infrastructure that runs it (developer tools and APIs - application programming interfaces) as well as new security features.

REFERENCES

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

National Vulnerability Database: CVE-2020-1350
https://nvd.nist.gov/vuln/detail/CVE-2020-1350

Talos Rules 2020-07-14

https://snort.org/advisories/talos-rules-2020-07-14

Adobe Security Bulletin
https://helpx.adobe.com/security/products/media-encoder/apsb20-36.html

CVE-2020-9688
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9688

CVE-2020-9646
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9646
CVE-2020-9650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9650

CVE-2020-9682
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9682

Oracle July 2020 Security Bulletin
https://www.oracle.com/security-alerts/cpujul2020.html

Businesses Running Oracle: Get Ready for a Massive, Critical Patching Session
https://www.cbronline.com/news/oracle-patch-update

Cisco Security Advisories
https://tools.cisco.com/security/center/publicationListing.x

Cisco patches critical flaws in VPN routers and firewalls
https://www.helpnetsecurity.com/2020/07/17/cisco-patches-vpn-routers/

Cisco fixes critical pre-auth flaws allowing router takeover
https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-pre-auth-flaws-allowing-router-takeover/

New in Chrome 84
https://developers.google.com/web/updates/2020/07/nic84