Top Ten Most Current Exploits and Vulnerabilities

Divya T. Aradhya

Abstract

This paper explores the top ten exploits and vulnerabilities in Information Technology, in the recent times. It describes each exploit and lists the fixes and counterattacks, if present.

Keywords: software exploits, vulnerabilities, hacks, fixes, patches, cyber security

Top Ten Most Current Exploits and Vulnerabilities

The Information Technology realm is an exciting one. New innovations and new software being created almost every day, legacy systems being updated and spruced up, and in between these lies the grave world of possible exploits, vulnerabilities and crime. Roesch's (2015) web article talks about how the "evolving cyber threats and defenders' efforts to foil them defines today's cybersecurity arms race" and goes on to say that this race is in "full sprint mode". [1] Given this context, this paper attempts to compile an arguable list of the top ten exploits and vulnerabilities in recent times, by mainly referencing to the Common Vulnerability and Exposure website (http://cve.mitre.org/), the National Vulnerability Database (https://nvd.nist.gov/) and the individual vendor websites of the vulnerable software.

Top Ten Exploits

Each exploit on this list is one that was discovered in the recent past. A brief description of each vulnerability, the risks it poses (based on the C-I-A triad), and details of the availability of fixes or counterattacks follow.

#1: Python: Heap Overflow Vulnerability

When was it discovered/reported? January 21, 2016

What is it about? According to the National Vulnerability Database [2], the "integer overflow in the get_data function in zipimport.c in CPython (aka Python)" gives access to "remote attackers" on the network, to create havoc "via a negative data size value, which triggers a heap-based buffer overflow."

Threat to Information Confidentiality? Yes

Threat to Information Integrity? Yes

Threat to Information Availability? Yes

CVE Id: CVE-2016-5636

***Exploitation*:** No known/reported exploitations.

Known Fixes: It has been fixed in a patch released on June 24, 2016. [3]

#2: Adobe Acrobat and Reader: Buffer Over-flow Vulnerability

When was it discovered/reported? June, 2016

What is it about? According to the NVD website [4], "Unspecified vulnerability in the Oracle Secure Global Desktop component in Oracle Virtualization 4.63, 4.71, and 5.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to OpenSSL."

Threat to Information Confidentiality? Yes

Threat to Information Integrity? Yes

Threat to Information Availability? Yes

CVE Id: CVE-2016-3613

***Exploitation*:** No known/reported exploitations

Known Fixes: Fixed in the Oracle Critical Patch Update (July 2016). [5]

#3: vBulletin ForumRunner add-on: SQL Injection Vulnerability

When was it discovered/reported? June 16, 2016

What is it about? ForumRunner is a multi-forum add-on for mobile phones, which allows a user to access forums at high speed. According to the NVD website [6], ForumRunner has a

vulnerability which “allows remote attackers to execute arbitrary SQL commands via the postids parameter to forumrunner/request.php”.

Threat to Information Confidentiality? Yes

Threat to Information Integrity? Yes

Threat to Information Availability? Yes

CVE Id: CVE-2016-6195

***Exploitation*:** The vulnerability has been known to be exploited in the wild in July 2016.

Known Fixes: Patched in vBulletin 4.2.2 Patch Level 5 and also in vBulletin 4.2.3 Patch Level 1. [7]

#4: ReadyDesk: Multiple Critical Vulnerabilities

When was it discovered/reported? July, 2016

What is it about? According to the Vulnerability Notes Database [8], ReadyDesk is “a help desk ticketing web application designed to facilitate business internal or business to customer interactions” and version 9.1 contains several security critical vulnerabilities including those of SQL injections and arbitrary file uploads. [9] It further reports that “A remote, unauthenticated attacker can obtain sensitive database information, read arbitrary files, and execute arbitrary code in the context of the vulnerable software.”

Threat to Information Confidentiality? Yes

Threat to Information Integrity? Yes

Threat to Information Availability? Yes

CVE Id: CVE-2016-5050

***Exploitation*:** No known/reported exploitations.

Known Fixes: On July 16, 2016, ReadyDesk released version 9.2 stating that it consisted of "Critical Security Updates" [10] but it did not specifically address if these vulnerabilities had been fixed.

#5: Adobe Acrobat and Reader: Buffer Over-flow Vulnerability

When was it discovered/reported? July 7, 2016

What is it about? According to the NVD website [11], Adobe Acrobat and Reader have vulnerabilities resulting from buffer overflow errors which allow malicious users on the network to execute arbitrary code which can take over the user's system.

Threat to Information Confidentiality? Yes

Threat to Information Integrity? Yes

Threat to Information Availability? Yes

CVE Id: CVE-2016-4270

Exploitation**:** No known/reported exploitations

Known Fixes: Adobe has released security updates for Adobe Acrobat and Reader for Windows and Macintosh (11.0.17). [12]

#6: vBulletin: Server-side Request Forgery (SSRF) Vulnerability

When was it discovered/reported? August 1, 2016

What is it about? An existing flaw in the design of the media-file upload module allows a use to launch a SSRF attack over the network, as a maliciously-crafted input URL results in a Redirection HTTP status code. [13]

Threat to Confidentiality? No

Threat to Integrity? Yes

Threat to Availability? No

CVE Id: CVE-2016-6483

***Exploitation*:** No known/reported exploitations.

Known Fixes: It has been fixed in security patch 5.2.2 and is part of the 5.2.3 vBulletin release. [14]

#7: Address Bar (Omni-bar) Spoofing in Mozilla for Android

When was it discovered/reported? August 2, 2016

What is it about? Firefox for Android has a flaw in processing Hebrew/Arabic text and can be manipulated to be redirected, as the URL sections get "flipped".

Baloch (2016) [15]is his Proof of Concept shows -

Input to browser in the Omni bar: http://امارات.عربي/google.com/test/test/test

Output from the Omni bar: http://google.com/test/test/test/امارات.عربي/

The Mozilla website states that this flaw "can be used to cause only certain portions of the loaded left-to-right character portion of the URL to be displayed, misleading users as to what site is loaded, possibly leading to phishing attacks." [16]

Threat to Information Confidentiality? No

Threat to Information Integrity? Yes

Threat to Information Availability? No

CVE Id: CVE-2016-5267 [17]

***Exploitation*:** No known/reported exploitations.

Known Fixes: Mozilla fixed it in Firefox 48

#8: NUUO and Netgear: Multiple Critical Vulnerabilities

When was it discovered/reported? August 4, 2016

What is it about? According to the Vulnerability Notes Database [18], "NUUO NVRmini 2, NVRsolo, Crystal, and Netgear ReadyNAS Surveillance products have web management interfaces containing multiple vulnerabilities that can be leveraged to gain complete control of affected devices." The interfaces give access to remote attackers and lets them custom PHP code via the log parameter. The flaws are varied are attributed to hidden pages, hard-coded credentials, improper validation and authentication, and buffer overflow issues.

Threat to Information Confidentiality? Yes

Threat to Information Integrity? Yes

Threat to Information Availability? Yes

CVE Id: CVE-2016-5674

***Exploitation*:** No known/reported exploitations.

Known Fixes: There are no known fixes, and Netgear has admitted that it is "currently unaware of a practical solution to this problem" and that a possible workaround can be "a general good security practice" and that the user should "only allow connections from trusted hosts and networks." [19]

#9: VMware Identity Manager & vRealize Automation: Critical Security Vulnerabilities

When was it discovered/reported? August 23, 2016

What is it about? According to the VMware security pages [20], VMware Identity Manager and vRealize Automation contain a flaw which makes them vulnerable to network

attacks. A malicious user can login into a low-privileged account and exploit the flaw and gain escalated root privileges.

Threat to Information Confidentiality? Yes

Threat to Information Integrity? Yes

Threat to Information Availability? Yes

CVE Id: CVE-2016-5336 [21]

***Exploitation*:** No known/reported exploitations.

Known Fixes: Patched in VMware Identity Manager 2.7 and vRealize Automation 7.1

#10: Cisco Small Business: Denial of Service Vulnerability

When was it discovered/reported? August 31, 2016

What is it about? A user with malicious intent can bombard the web-based management interface of Cisco Small Business 220 Series Smart Plus (Sx220) Switches through custom HTTP requests, and potentially trigger a Denial-of-Service attack. The Cisco Security website reports that "the vulnerability is due to insufficient validation of HTTP requests by the web-based management interface of an affected device." This exploit does not require authentication, and it allows disruption of service. [22]

Threat to Information Confidentiality? No

Threat to Information Integrity? No

Threat to Information Availability? Yes

CVE Id: CVE-2016-1472

***Exploitation*:** No known/reported exploitations.

Known Fixes: It has been fixed a subsequent software update. [23]

Conclusions

The list of software vulnerabilities grows with each minute and can prove to provide grave risks to the security of data and information, as they open themselves up to malicious exploitation which affect their confidentiality, integrity and availability.

Having a vigilant team of designers, developers, testers and bounty-hunting ethical hackers can possibly give an edge in the race against the crackers.

References

[1] @. (n.d.). The Industrialization of Hacking. Retrieved September 04, 2016, from https://newsroom.cisco.com/feature-content?articleId=1572627

[2] (n.d).(n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5636

[3] Issue 26171: Heap overflow in zipimporter module - Python tracker. (n.d.). Retrieved from https://bugs.python.org/issue26171

[4] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3613

[5] Oracle Critical Patch Update - July 2016. (n.d.). Retrieved from http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html

[6] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6195

[7] The Official vBulletin Modifications Site. (n.d.). Retrieved from http://www.vbulletin.org/forum/showthread.php?t=322848

[8] (n.d).https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5050

[9] Vulnerability Note VU#294272. (n.d.). Retrieved from http://www.kb.cert.org/vuls/id/294272

[10] Help Desk Software, Live Chat Software, Remote Desktop. (n.d.). Retrieved from http://readydesk.com/news.asp?ID=88

[11] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4270

[12] Adobe Security Bulletin. (n.d.). Retrieved from https://helpx.adobe.com/security/products/acrobat/apsb16-26.html

[13] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6483

[14] Wayne Luke vBulletin Technical Support Lead Join Date: Aug 2000 Posts: 54950. (n.d.). Announcement. Retrieved from http://www.vbulletin.com/forum/forum/vbulletin-

announcements/vbulletin-announcements_aa/4349551-security-patch-vbulletin-5-2-0-5-2-1-5-2-2

[15] Baloch, R. (2016, September 04). Google Chrome, Firefox Address Bar Spoofing Vulnerability. Retrieved from http://www.rafayhackingarticles.net/2016/08/google-chrome-firefox-address-bar.html

[16] Addressbar spoofing with right-to-left characters on Firefox for Android. (n.d.). Retrieved from https://www.mozilla.org/en-US/security/advisories/mfsa2016-82/

[17] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5267

[18] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5674

[19] Vulnerability Note VU#856152. (n.d.). Retrieved from http://www.kb.cert.org/vuls/id/856152

[20] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5336

[21] VMSA-2016-0013. (n.d.). Retrieved from http://www.vmware.com/security/advisories/VMSA-2016-0013.html

[22] (n.d). https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1472

[23] Cisco Security. (n.d.). Retrieved from https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps2