Awesome CVE PoC

hades / 2017-04-24 02:19:04 / 浏览数 4330 安全工具 工具 顶(0) 踩(0)

Awesome CVE PoC

Here is a collection about Proof of Concepts of Common Vulnerabilities and Exposures.

Please read the contribution guidelines before contributing.

Contents

- CVE-2017-0392
- CVE-2017-0521
- CVE-2017-0531
- CVE-2017-0576
- CVE-2017-2416
- CVE-2017-2446
- CVE-2017-2447
- CVE-2017-2464
- CVE-2017-2636
- CVE-2017-5638
- CVE-2017-7280

Resource

CVE-2013-6632

- Integer overflow in Google Chrome before 31.0.1650.57 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013.

CVE-2014-1705

- Google V8, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

CVE-2014-3176

- Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3177.

CVE-2014-7927

- The SimplifiedLowering::DoLoadBuffer function in compiler/simplified-lowering.cc in Google V8, as used in Google Chrome before 40.0.2214.91, does not properly choose an integer data type, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2014-7928

- hydrogen.cc in Google V8, as used Google Chrome before 40.0.2214.91, does not properly handle arrays with holes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers an array copy.

CVE-2015-0235

- Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST".

CVE-2015-1233

- Google Chrome before 41.0.2272.118 does not properly handle the interaction of IPC, the Gamepad API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors.

CVE-2015-1242

- The ReduceTransitionElementsKind function in hydrogen-check-elimination.cc in Google V8 before 4.2.77.8, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that leverages "type confusion" in the check-elimination optimization.

CVE-2015-3306

- The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

CVE-2015-6764

- The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2015-6771

- js/array.js in Google V8, as used in Google Chrome before 47.0.2526.73, improperly implements certain map and filter operations for arrays, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2015-7545

- The (1) git-remote-ext and (2) unspecified other remote helper programs in Git before 2.3.10, 2.4.x before 2.4.10, 2.5.x before 2.5.4, and 2.6.x before 2.6.1 do not properly restrict the allowed protocols, which might allow remote attackers to execute arbitrary code via a URL in a (a) .gitmodules file or (b) unknown other sources in a submodule.

CVE-2015-8584

- JSON, OOB.

CVE-2016-0728

- The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted keyctl commands.

CVE-2016-1646

- The Array.prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2016-1653

- The LoadBuffer implementation in Google V8, as used in Google Chrome before 50.0.2661.75, mishandles data types, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc.

CVE-2016-1665

- The JSGenericLowering class in compiler/js-generic-lowering.cc in Google V8, as used in Google Chrome before 50.0.2661.94, mishandles comparison operators, which allows remote attackers to obtain sensitive information via crafted JavaScript code.

CVE-2016-1669

- The Zone::New function in zone.cc in Google V8 before 5.0.71.47, as used in Google Chrome before 50.0.2661.102, does not properly determine when to expand certain memory allocations, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2016-1677

- uri.js in Google V8 before 5.1.281.26, as used in Google Chrome before 51.0.2704.63, uses an incorrect array type, which allows remote attackers to obtain sensitive information by calling the decodeURI function and leveraging "type confusion".

CVE-2016-1688

- The regexp (aka regular expression) implementation in Google V8 before 5.0.71.40, as used in Google Chrome before 51.0.2704.63, mishandles external string sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted JavaScript code.

CVE-2016-1857

- WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1856.

CVE-2016-4622

- WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4623, and CVE-2016-4624.

CVE-2016-4734

- WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4735.

CVE-2016-3386

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3389,

CVE-2016-7190, and CVE-2016-7194.

CVE-2016-5129

- Google V8 before 5.2.361.32, as used in Google Chrome before 52.0.2743.82, does not properly process left-trimmed objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2016-5172

- The parser in Google V8, as used in Google Chrome before 53.0.2785.113, mishandles scopes, which allows remote attackers to obtain sensitive information from arbitrary memory locations via crafted JavaScript code.

CVE-2016-5198

- V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.

CVE-2016-5200

- V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2016-7189

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Remote Code Execution Vulnerability".

CVE-2016-7190

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3386, CVE-2016-3389, and CVE-2016-7194.

CVE-2016-7194

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3386, CVE-2016-3389, and CVE-2016-7190.

CVE-2016-7200

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7201

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7202

- The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," as demonstrated by the Chakra JavaScript engine, a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7203

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7240

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7241

- Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability".

CVE-2016-7286

- The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7288, CVE-2016-7296, and CVE-2016-7297.

CVE-2016-7287

- The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability".

CVE-2016-7288

- The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7296, and CVE-2016-7297.

CVE-2016-8413

- An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32709702. References: QC-CR#518731.

CVE-2016-8477

- An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32720522. References: QC-CR#1090007.

CVE-2016-9651

- RESERVED This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-0070

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

CVE-2017-0071

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

CVE-2017-0199

- Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."

CVE-2017-0392

- A denial of service vulnerability in VBRISeeker.cpp in libstagefright in Mediaserver could enable a remote attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1. Android ID: A-32577290.

CVE-2017-0521

- An elevation of privilege vulnerability in the Qualcomm camera driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32919951. References: QC-CR#1097709.

CVE-2017-0531

- An information disclosure vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32877245. References: QC-CR#1087469.

CVE-2017-0576

- An elevation of privilege vulnerability in the Qualcomm crypto engine driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33544431. References: QC-CR#1103089.

CVE-2017-2416

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted image file.

CVE-2017-2446

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages the mishandling of strict mode functions.

CVE-2017-2447

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a crafted web site.

CVE-2017-2464

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2636

- Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.

CVE-2017-5638

- The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.

CVE-2017-7280

- An issue was discovered in api/includes/systems.php in Unitrends Enterprise Backup before 9.0.0. User input is not properly filtered before being sent to a popen function. This allows for remote code execution by sending a specially crafted user variable.

上一篇：TechSmith Camtasi... 下一篇：饿了么第一届信息安全峰会内容分享

1. 0 条回复
   - 动动手指，沙发就是你的了！

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板