PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Linux Kernel 4.13 - 4.16.11 Unspecified Vulnerability due to Out of Bounds memcpy - CVE-2018-11412	In the Linux kernel 4.13 through 4.16.11, ext4_read_inline_data() in fs/ext4/inline.c performs a memcpy with an untrusted length value in certain circumstances involving a crafted filesystem that stores the system.data extended attribute value in a dedicated inode.	Version(s): <= 4.13 - 4.16.11	Published - May 24, 2018 CVE-2018-11412 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11412 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-11412
Events Calendar Plugin for WordPress Remote SQL Injection and XSS Vulnerability	Events Calendar plugin version 1.0 for WordPress is prone to a remote sql injection vulnerability. Cross-site scripting attacks are also possible. This vulnerability was published by ExploitDB	Version(s): <= 1.0	Published - May 27, 2018 SBV-85741 CVSS - 9.1 Vendor's Advisory - https://0day.asia/wordpress-0day-176263 https://www.exploit-db.com/exploits/44785/
TP-Link TL-WR840N and TL-WR841N Remote Authentication Bypass Vulnerability	TP-Link TL-WR840N and TL-WR841N are prone to a remote authentication bypass vulnerability. A remote attacker could exploit this issue by sending Referrer Header with its request and setting Referrer: http://192.168.0.1/mainFrame.htm. This vulnerability was published by ExploitDB	Version(s): <= 0.9.1_4.16_v0001.0_Build_170622_Rel.64334n, 0.9.1_3.16_v0001.0_Build_170608_Rel.58696n	Published - May 29, 2018 SBV-85737 CVSS - 9.8 Vendor's Advisory - https://0day.asia/tp-link-0day-176261 https://www.exploit-db.com/exploits/44781/
dalek-browser-chrome-canary Remote Code Execution Vulnerability - CVE-2016-10584	dalek-browser-chrome-canary provides Google Chrome bindings for DalekJS. All versions of dalek-browser-chrome-canary downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.	Version(s): <= *	Published - May 29, 2018 CVE-2018-10584 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10584 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10584
ibm_db Remote Code Execution Vulnerability - CVE-2016-10577	ibm_db is an asynchronous/synchronous interface for node.js to IBM DB2 and IBM Informix. ibm_db before 1.0.2 downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.	Version(s): <= 1.0.2	Published - May 29, 2018 CVE-2018-10577 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10577 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10577
MULTIDOTS Woo Checkout for Digital Goods plugin 2.1 for WordPress CSRF Vulnerability - CVE-2018-11633	An issue was discovered in the MULTIDOTS Woo Checkout for Digital Goods plugin 2.1 for WordPress. If an admin user can be tricked into visiting a crafted URL created by an attacker (via spear phishing/social engineering), the attacker can change the plugin settings. The function woo_checkout_settings_page in the file class-woo-checkout-for-digital-goods-admin.php doesn't do any check against wp-admin/admin-post.php Cross-site request forgery (CSRF) and user capabilities	Version(s): <= 2.1	Published - May 31, 2018 CVE-2013-11633 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11633 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-11633
Bitty Directory Traversal Vulnerability - CVE-2016-10561	Bitty is a development web server tool that functions similar to `python -m SimpleHTTPServer`. Version 0.2.10 has a directory traversal vulnerability that is exploitable via the URL path in GET requests.	Version(s): < 0.2.10	Published - May 31, 2018 CVE-2018-10561 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10561 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10561
mongoDB Man-in-the-Middle or Remote Code Execution Vulnerability - CVE-2016-10572	mongodb-instance before 0.0.3 installs mongodb locally. mongodb-instance downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.	Version(s): <= 0.0.3	Published - May 31, 2018 CVE-2018-10572 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10572 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10572
Adobe AIR SDK Man-in-the-Middle or Remote Code Execution Vulnerability - CVE-2016-10603	air-sdk is a NPM wrapper for the Adobe AIR SDK. air-sdk downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.	Version(s): <=*	Published - June 01, 2018 CVE-2016-10603 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10603 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10603
Selenium Chromedriver Man-in-the-Middle or Remote Code Execution Vulnerability - CVE-2016-10624	selenium-chromedriver is a simple utility for downloading the Selenium Webdriver for Google Chrome selenium-chromedriver downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.	Version(s): <= *	Published - June 01, 2018 CVE-2016-10624 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10624 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10624
bkjs-wand <0.3.2 Local Network Code Execution Vulnerability - CVE-2016-10571	bkjs-wand versions lower than 0.3.2 download binary resources over HTTP, which leaves them vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.	Version(s): <= 0.3.2	Published - May 31, 2018 CVE-2016-10571 CVSS - 7.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10571 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10571
ImageMagick 7.0.7-37 Q16 - Heap Buffer Overread via Crafted File - CVE-2018-11625	In ImageMagick 7.0.7-37 Q16, SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer over-read via a crafted file.	Version(s): <= 7.0.7\-36 Q16	Published - May 31, 2018 CVE-2018-11625 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11625 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-11625