Vulnerability Summary for the Week of June 19, 2017

Please Note:

• The vulnerabilities are categorized by their level of severity which is either High, Medium or Low.

• The CVE identity number is the publicly known ID given to that particular vulnerability. Therefore, you can search the status of that particular vulnerability using that ID.

• The CVSS (Common Vulnerability Scoring System) score is a standard scoring system used to determine the severity of the vulnerability.

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
adobe -- captivate	Adobe Captivate versions 9 and earlier have a remote code execution vulnerability in the quiz reporting feature that could be abused to read and write arbitrary files to the server.	2017-06-20	10.0	CVE-2017-3098 CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF runtime engine. Successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3088 BID(link is external) CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF imaging model. Successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3089 BID(link is external) CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the bitmap representation module. Successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3093 BID(link is external) CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF processing engine.	2017-06-20	10.0	CVE-2017-3094 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Successful exploitation could lead to arbitrary code execution.			CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF parsing engine. Successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3095 BID(link is external) CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the character code mapping module. Successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3096 BID(link is external) CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier contain an insecure library loading vulnerability. The vulnerability is due to unsafe library loading functions in the installer plugin. A successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3097 BID(link is external) CONFIRM(link is external)
adobe -- flash_player	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in the Primetime SDK functionality related to the profile metadata of the media stream. Successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3083 BID(link is external) CONFIRM(link is external)
adobe -- flash_player	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in the advertising metadata functionality. Successful exploitation could lead to arbitrary code execution.	2017-06-20	10.0	CVE-2017-3084 BID(link is external) CONFIRM(link is external)
nuevomailer -- nuevomailer	SQL injection vulnerability in rdr.php in nuevoMailer version 6.0 and earlier allows remote attackers to execute arbitrary SQL commands via the "r" parameter.	2017-06-19	7.5	CVE-2017-9730 EXPLOIT-DB(link is external)
uclibc -- uclibc	In uClibc 0.9.33.2, there is an out-of-bounds read in the get_subexp function in misc/regex/regexec.c when processing a crafted regular expression.	2017-06-16	7.5	CVE-2017-9728 MISC(link is external)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- captivate	Adobe Captivate versions 9 and earlier have an information disclosure vulnerability resulting from abuse of the quiz reporting feature in Captivate.	2017-06-20	5.0	CVE-2017-3087 CONFIRM(link is external)
apache -- thrift	The client libraries in Apache Thrift before 0.9.3 might allow remote authenticated users to cause a denial of service (infinite recursion) via vectors involving the skip function.	2017-06-16	4.0	CVE-2015-3254 CONFIRM(link is external) BID(link is external) CONFIRM MLIST
cmsmadesimple -- cms_made_simple	In admin\addgroup.php in CMS Made Simple 2.1.6, when adding a user group, there is no XSS filtering, resulting in storage-type XSS generation, via the description parameter in an addgroup action.	2017-06-18	4.3	CVE-2017-9668 MISC(link is external)
uclibc -- uclibc	In uClibc 0.9.33.2, there is stack exhaustion (uncontrolled recursion) in the check_dst_limits_calc_pos_1 function in misc/regex/regexec.c when processing a crafted regular expression.	2017-06-16	5.0	CVE-2017-9729 MISC(link is external)
zenbership -- zenbership	SQL Injection exists in admin/index.php in Zenbership 1.0.8 via the filters array parameter, exploitable by a privileged account.	2017-06-19	6.5	CVE-2017-9759 BID(link is external) MISC(link is external)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e.,	2017-06-17	2.1	CVE-2017-1000380 MISC MISC MISC MISC(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time.			external) BID(link is external) MISC(link is external) MISC(link is external)
qemu -- qemu	Memory leak in QEMU (aka Quick Emulator), when built with IDE AHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the AHCI device.	2017-06-16	1.9	CVE-2017-9373 CONFIRM MLIST(link is external) BID(link is external) CONFIRM(link is external)
qemu -- qemu	Memory leak in QEMU (aka Quick Emulator), when built with USB EHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the device.	2017-06-16	2.1	CVE-2017-9374 CONFIRM MLIST(link is external) CONFIRM(link is external)
qemu -- qemu	QEMU (aka Quick Emulator), when built with USB xHCI controller emulator support, allows local guest OS privileged users to cause a denial of service (infinite recursive call) via vectors involving control transfer descriptors sequencing.	2017-06-16	1.9	CVE-2017-9375 CONFIRM MLIST(link is external) BID(link is external) CONFIRM(link is external)
qemu -- qemu	QEMU (aka Quick Emulator), when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest OS privileged users to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving megasas command processing.	2017-06-16	1.9	CVE-2017-9503 MLIST(link is external) BID(link is external) CONFIRM(link is external) MLIST MLIST

Severity Not Yet Assigned				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
acronis_international -- true_image	Acronis True Image up to and including version 2017 Build 8053 performs software updates using HTTP. Downloaded updates are only verified using a server-provided MD5 hash.	2017-06-21	not yet calculated	CVE-2017-3219 BID(link is external) CERT-VN
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier contain an insecure library loading vulnerability. The vulnerability is due to unsafe library loading of editor control library functions in the installer plugin. A successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3092 BID(link is external) CONFIRM(link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.4 and earlier contain an insecure library loading vulnerability. The vulnerability is due to unsafe library loading of browser related library extensions in the installer plugin. A successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3090 BID(link is external) CONFIRM(link is external)
adobe -- flash	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability during internal computation caused by multiple display object mask manipulations. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3081 BID(link is external) CONFIRM(link is external)
adobe -- flash	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the PNG image parser. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3077 BID(link is external) CONFIRM(link is external)
adobe -- flash	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the internal representation of raster data. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3079 BID(link is external) CONFIRM(

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				link is external)
adobe -- flash	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the MPEG-4 AVC module. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3076 BID(link is external) CONFIRM(link is external)
adobe -- flash	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the Adobe Texture Format (ATF) module. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3078 BID(link is external) CONFIRM(link is external)
adobe -- flash	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability when manipulating the ActionsScript 2 XML class. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3075 BID(link is external) CONFIRM(link is external)
adobe -- flash	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the LocaleID class. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3082 BID(link is external) CONFIRM(link is external)
adobe -- shockwave	Adobe Shockwave versions 12.2.8.198 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-06-20	not yet calculated	CVE-2017-3086 BID(link is external) CONFIRM(link is external)
apache -- hpptd	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of	2017-06-19	not yet calculated	CVE-2017-7668 BID(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.			external) MLIST
apache -- hpptd	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	2017-06-19	not yet calculated	CVE-2017-7679 BID(link is external) MLIST
apache -- httpd	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	2017-06-19	not yet calculated	CVE-2017-3169 BID(link is external) MLIST
apache -- httpd	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	2017-06-19	not yet calculated	CVE-2017-3167 BID(link is external) MLIST
apcupsd -- apcupsd	In Adam Kropelin adk0212 APC UPS Daemon through 3.14.14, the default installation of APCUPSD allows a local authenticated, but unprivileged, user to run arbitrary code with elevated privileges by replacing the service executable apcupsd.exe with a malicious executable that will run with SYSTEM privileges at startup. This occurs because of "RW NT AUTHORITY\Authenticated Users" permissions for %SYSTEMDRIVE%\apcupsd\bin\apcupsd.exe.	2017-06-16	not yet calculated	CVE-2017-7884 MISC BID(link is external)
binutils -- binutils	opcodes/rx-decode.opc in GNU Binutils 2.28 lacks bounds checks for certain scale arrays, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by	2017-06-19	not yet calculated	CVE-2017-9750 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mishandling of this file during "objdump -D" execution.			
binutils -- binutils	The ieee_object_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.	2017-06-19	not yet calculated	CVE-2017-9748 BID(link is external) CONFIRM
binutils -- binutils	The ieee_archive_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.	2017-06-19	not yet calculated	CVE-2017-9747 BID(link is external) CONFIRM
binutils -- binutils	The *regs* macros in opcodes/bfin-dis.c in GNU Binutils 2.28 allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9749 BID(link is external) CONFIRM
binutils -- binutils	The versados_mkobject function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not initialize a certain data structure, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as	2017-06-19	not yet calculated	CVE-2017-9753 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	demonstrated by mishandling of this file during "objdump -D" execution.			
binutils -- binutils	The process_otr function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not validate a certain offset, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9754 BID(link is external) CONFIRM
binutils -- binutils	opcodes/i386-dis.c in GNU Binutils 2.28 does not consider the number of registers for bnd mode, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9755 BID(link is external) CONFIRM
binutils -- binutils	The aarch64_ext_ldst_reglist function in opcodes/aarch64-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9756 BID(link is external) CONFIRM
binutils -- binutils	The disassemble_bytes function in objdump.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of rae insns printing for this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9746 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
binutils -- binutils	The score_opcodes function in opcodes/score7-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9742 BID(link is external) CONFIRM
binutils -- binutils	The print_insn_score32 function in opcodes/score7-dis.c:552 in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9743 BID(link is external) MISC
binutils -- binutils	opcodes/rl78-decode.opc in GNU Binutils 2.28 has an unbounded GETBYTE macro, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9751 BID(link is external) CONFIRM
binutils -- binutils	The sh_elf_set_mach_from_flags function in bfd/elf32-sh.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9744 BID(link is external) CONFIRM
binutils -- binutils	The _bfd_vms_slurp_etir function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application	2017-06-19	not yet calculated	CVE-2017-9745 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.			
binutils -- binutils	bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file in the _bfd_vms_get_value and _bfd_vms_slurp_etir functions during "objdump -D" execution.	2017-06-19	not yet calculated	CVE-2017-9752 BID(link is external) CONFIRM
boa_webserver -- boa_webserver	/cgi-bin/wapopen in BOA Webserver 0.94.14rc21 allows the injection of "../.." using the FILECAMERA variable (sent by GET) to read files with root privileges.	2017-06-23	not yet calculated	CVE-2017-9833 MISC(link is external)
bornfromfire -- android_kernel_huawei_msm8916	The msm_bus_dbg_update_request_write function in drivers/platform/msm/msm_bus/msm_bus_dbg.c in android_kernel_huawei_msm8916 through 2017-06-16 in LineageOS, and possibly other kernels for MSM devices, allows attackers to cause a denial of service (NULL pointer dereference and device crash) via a crafted /sys/kernel/debug/msm-bus-dbg/client-data/update-request write request.	2017-06-16	not yet calculated	CVE-2017-6899 MISC(link is external) BID(link is external)
breezejs -- breeze.server.net	IdeaBlade Breeze Breeze.Server.NET before 1.6.5 allows remote attackers to execute arbitrary code, related to use of TypeNameHandling in JSON deserialization.	2017-06-22	not yet calculated	CVE-2017-9424 MISC(link is external) MISC(link is external)
cambium_networks -- epmp	An Improper Access Control issue was discovered in Cambium Networks ePMP. After a valid user has used SNMP configuration export, an attacker is able to remotely trigger device configuration backups using specific MIBs. These	2017-06-21	not yet calculated	CVE-2017-7918 BID(link is external) MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	backups lack proper access control and may allow access to sensitive information and possibly allow for configuration changes.			
cambium_networks -- epmp	An Improper Privilege Management issue was discovered in Cambium Networks ePMP. The privileges for SNMP community strings are not properly restricted, which may allow an attacker to gain access to sensitive information and possibly allow for configuration changes.	2017-06-21	not yet calculated	CVE-2017-7922 BID(link is external) MISC
check_mk -- check_mk	A cross site scripting (XSS) vulnerability exists in Check_MK versions 1.4.0x prior to 1.4.0p6, allowing an unauthenticated remote attacker to inject arbitrary HTML or JavaScript via the _username parameter when attempting authentication to webapi.py, which is returned unencoded with content type text/html.	2017-06-21	not yet calculated	CVE-2017-9781 CONFIRM(link is external)
easysite -- webservices	SQL injection vulnerability in C_InfoService.asmx in WebServices in Easysite 7.0 could allow remote attackers to execute arbitrary SQL commands via an XML document containing a crafted ArticleIDs element within a GetArticleHitsArray element.	2017-06-24	not yet calculated	CVE-2017-9848 MISC(link is external)
ecava -- integraxor	A SQL Injection issue was discovered in Ecava IntegraXor Versions 5.2.1231.0 and prior. The application fails to properly validate user input, which may allow for an unauthenticated attacker to remotely execute arbitrary code in the form of SQL queries.	2017-06-21	not yet calculated	CVE-2017-6050 BID(link is external) MISC
elastic -- kibana	Kibana before 4.5.4 and 4.1.11 are vulnerable to an XSS attack that would allow an attacker to execute arbitrary JavaScript in users' browsers.	2017-06-16	not yet calculated	CVE-2016-1000220 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- kibana	Kibana before 4.5.4 and 4.1.11 when a custom output is configured for logging in, cookies and authorization headers could be written to the log files. This information could be used to hijack sessions of other users when using Kibana behind some form of authentication such as Shield.	2017-06-16	not yet calculated	CVE-2016-1000219 BID(link is external) CONFIRM(link is external)
elastic -- logstach	Logstash prior to version 2.3.4, Elasticsearch Output plugin would log to file HTTP authorization headers which could contain sensitive information.	2017-06-16	not yet calculated	CVE-2016-1000221 BID(link is external) CONFIRM(link is external)
elastic -- logstach	Prior to Logstash version 5.0.1, Elasticsearch Output plugin when updating connections after sniffing, would log to file HTTP basic auth credentials.	2017-06-16	not yet calculated	CVE-2016-10362 BID(link is external) CONFIRM(link is external)
ellislab -- expressionengine	ExpressionEngine version 2.x < 2.11.8 and version 3.x < 3.5.5 create an object signing token with weak entropy. Successfully guessing the token can lead to remote code execution.	2017-06-22	not yet calculated	CVE-2017-0897 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) MISC(link is external)
emc_corportation -- isilon_onefs	EMC Isilon OneFS 8.0.1.0, 8.0.0 - 8.0.0.3, 7.2.0 - 7.2.1.4, 7.1.x is affected by a privilege escalation vulnerability that could potentially be exploited by attackers to compromise the affected system.	2017-06-21	not yet calculated	CVE-2017-4988 CONFIRM(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
emc_corportation -- vavamar_server_software	In EMC Avamar Server Software 7.4.1-58, 7.4.0-242, 7.3.1-125, 7.3.0-233, 7.3.0-226, an unauthorized attacker may leverage the file upload feature of the system maintenance page to load a maliciously crafted file to any directory which could allow the attacker to execute arbitrary code on the Avamar Server system.	2017-06-21	not yet calculated	CVE-2017-4990 CONFIRM(link is external)
emc_corportation -- vavamar_server_software	In EMC Avamar Server Software 7.3.1-125, 7.3.0-233, 7.3.0-226, 7.2.1-32, 7.2.1-31, 7.2.0-401, an unauthenticated remote attacker may potentially bypass the authentication process to gain access to the system maintenance page. This may be exploited by an attacker to view sensitive information, perform software updates, or run maintenance workflows.	2017-06-21	not yet calculated	CVE-2017-4989 CONFIRM(link is external)
emc_corportation -- vnx	In EMC VNX2 versions prior to OE for File 8.1.9.211 and VNX1 versions prior to OE for File 7.1.80.8, a local authenticated user can load a maliciously crafted file in the search path which may potentially allow the attacker to execute arbitrary code on the targeted VNX Control Station system, aka an uncontrolled search path vulnerability.	2017-06-19	not yet calculated	CVE-2017-4987 CONFIRM(link is external) BID(link is external)
emc_corportation -- vnx	In EMC VNX2 versions prior to OE for File 8.1.9.211 and VNX1 versions prior to OE for File 7.1.80.8, a local authenticated user may potentially escalate their privileges to root due to authorization checks not being performed on certain perl scripts. This may potentially be exploited by an attacker to run arbitrary commands as root on the targeted VNX Control Station system.	2017-06-19	not yet calculated	CVE-2017-4985 CONFIRM(link is external) BID(link is external)
emc_corportation -- vnx	In EMC VNX2 versions prior to OE for File 8.1.9.211 and VNX1 versions prior to OE for File 7.1.80.8, an unauthenticated remote attacker may be able to elevate their permissions to root through a command injection. This may potentially be exploited	2017-06-19	not yet calculated	CVE-2017-4984 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by an attacker to run arbitrary code with root-level privileges on the targeted VNX Control Station system, aka remote code execution.			BID(link is external)
exim -- exim	Exim supports the use of multiple "-p" command line arguments which are malloc()'ed and never free()'ed, used in conjunction with other issues allows attackers to cause arbitrary code execution. This affects exim version 4.89 and earlier. Please note that at this time upstream has released a patch (commit 65e061b76867a9ea7aeeb535341b790b90ae6c21), but it is not known if a new point release is available that addresses this issue at this time.	2017-06-19	not yet calculated	CVE-2017-1000369 CONFIRM(link is external) MISC(link is external) MISC(link is external)
faac_project -- freeware_advanced_audio_coder	The faacEncOpen function in libfaac/frame.c in Freeware Advanced Audio Coder (FAAC) 1.28 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted wav file.	2017-06-21	not yet calculated	CVE-2017-9130 EXPLOIT-DB(link is external)
faac_project -- freeware_advanced_audio_coder	The wav_open_read function in frontend/input.c in Freeware Advanced Audio Coder (FAAC) 1.28 allows remote attackers to cause a denial of service (large loop) via a crafted wav file.	2017-06-21	not yet calculated	CVE-2017-9129 EXPLOIT-DB(link is external)
flatpak -- flatpak	In Flatpak before 0.8.7, a third-party app repository could include malicious apps that contain files with inappropriate permissions, for example setuid or world-writable. The files are deployed with those permissions, which would let a local attacker run the setuid executable or write to the world-writable location. In the case of the "system helper" component, files deployed as part of the app are owned by root, so in the worst case they could be setuid root.	2017-06-21	not yet calculated	CVE-2017-9780 CONFIRM CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foscam -- c1	Hard-coded FTP credentials (r:r) are included in the Foscam C1 running firmware 1.9.1.12. Knowledge of these credentials would allow remote access to any cameras found on the internet that do not have port 50021 blocked by an intermediate device.	2017-06-21	not yet calculated	CVE-2016-8731 BID(link is external) MISC(link is external)
foscam -- c1	An exploitable command injection vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can allow for a user to inject arbitrary shell characters during account creation resulting in command injection. An attacker can simply send an HTTP request to the device to trigger this vulnerability.	2017-06-21	not yet calculated	CVE-2017-2827 BID(link is external) MISC(link is external)
foscam -- c1	An exploitable buffer overflow vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can cause a buffer overflow resulting in overwriting arbitrary data. An attacker can simply send an HTTP request to the device to trigger this vulnerability.	2017-06-21	not yet calculated	CVE-2017-2830 BID(link is external) MISC(link is external)
foscam -- c1	An exploitable directory traversal vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can cause the application to read a file from disk but a failure to adequately filter characters results in allowing an attacker to specify a file outside of a directory. An attacker can simply send an HTTP request to the device to trigger this vulnerability.	2017-06-21	not yet calculated	CVE-2017-2829 MISC(link is external)
foscam -- c1	An exploitable buffer overflow vulnerability exists in the web management interface used by the Foscam C1 Indoor	2017-06-21	not yet calculated	CVE-2017-2831 BID(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can cause a buffer overflow resulting in overwriting arbitrary data. An attacker can simply send an HTTP request to the device to trigger this vulnerability.			external) MISC(link is external)
foscam -- c1	An exploitable command injection vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can allow for a user to inject arbitrary shell characters during account creation resulting in command injection. An attacker can simply send an HTTP request to the device to trigger this vulnerability.	2017-06-21	not yet calculated	CVE-2017-2828 BID(link is external) MISC(link is external)
foscam -- c1	An exploitable stack-based buffer overflow vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera. A specially crafted http request can cause a stack-based buffer overflow resulting in overwriting arbitrary data on the stack frame. An attacker can simply send an http request to the device to trigger this vulnerability.	2017-06-21	not yet calculated	CVE-2017-2805 BID(link is external) MISC(link is external)
glpi_project -- glpi	Multiple SQL injection vulnerabilities in GLPI 0.90.4 allow an authenticated remote attacker to execute arbitrary SQL commands by using a certain character when the database is configured to use Big5 Asian encoding.	2017-06-21	not yet calculated	CVE-2016-7508 MISC(link is external)
gnu_project -- glibc	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they	2017-06-19	not yet calculated	CVE-2017-1000366 BID(link is external) CONFIRM(link is external) MISC(link is external) CONFIRM(

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	have not been given a CVE. This affects glibc 2.25 and earlier.			link is external) CONFIRM(link is external)
gnu_project -- gnu_debugger	GNU Debugger (GDB) 8.0 and earlier fails to detect a negative length field in a DWARF section. A malformed section in an ELF binary or a core file can cause GDB to repeatedly allocate memory until a process limit is reached. This can, for example, impede efforts to analyze malware with GDB.	2017-06-21	not yet calculated	CVE-2017-9778 CONFIRM
gnutls -- gnutls	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid contents. This could lead to a crash of the GnuTLS server application.	2017-06-16	not yet calculated	CVE-2017-7507 BID(link is external) CONFIRM
horde -- horde_image_2.x	Remote Code Execution was found in Horde_Image 2.x before 2.5.0 via a crafted GET request. Exploitation requires authentication.	2017-06-21	not yet calculated	CVE-2017-9774 CONFIRM
horde -- horde_image_2.x	Denial of Service was found in Horde_Image 2.x before 2.5.0 via a crafted URL to the "Null" image driver.	2017-06-21	not yet calculated	CVE-2017-9773 CONFIRM
ibm -- relm	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2017-06-22	not yet calculated	CVE-2016-9747 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- spectrum_scale/gpfs	IBM has identified a vulnerability with IBM Spectrum Scale/GPFS utilized on the Elastic Storage Server (ESS)/GPFS Storage Server (GSS) during testing of an unsupported configuration, where users applications are running on an active ESS	2017-06-21	not yet calculated	CVE-2017-1304 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	I/O server node and utilize direct I/O to perform a read or a write to a Spectrum Scale file. This vulnerability may result in the use of an incorrect memory address, leading to a Spectrum Scale/GPFS daemon failure with a Signal 11, and possibly leading to denial of service or undetected data corruption. IBM X-Force ID: 125458.			MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 could allow user to obtain sensitive information using an HTTP GET request. IBM X-Force ID: 123667.	2017-06-23	not yet calculated	CVE-2017-1193 CONFIRM(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 121418.	2017-06-23	not yet calculated	CVE-2017-1132 CONFIRM(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling File Gateway does not properly restrict user requests based on permission level. This allows for users to update data related to other users, by manipulating the parameters passed in the POST request. IBM X-Force ID: 126060.	2017-06-22	not yet calculated	CVE-2017-1326 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 could allow an authenticated user to obtain sensitive information by using unsupported, specially crafted HTTP commands. IBM X-Force ID: 121375.	2017-06-23	not yet calculated	CVE-2017-1131 CONFIRM(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 126462.	2017-06-23	not yet calculated	CVE-2017-1347 CONFIRM(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126524.	2017-06-23	not yet calculated	CVE-2017-1348 CONFIRM(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 115336.	2017-06-23	not yet calculated	CVE-2016-5893 CONFIRM(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 could allow a local user view sensitive information due to improper access controls. IBM X-Force ID: 125456.	2017-06-23	not yet calculated	CVE-2017-1302 CONFIRM(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 stores potentially sensitive information from HTTP sessions that could be read by a local user. IBM X-Force ID: 126525.	2017-06-23	not yet calculated	CVE-2017-1349 CONFIRM(link is external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 could allow an authenticated user with special privileges to view files that they should not have access to. IBM X-Force ID: 120275.	2017-06-22	not yet calculated	CVE-2016-9983 CONFIRM(link is external) BID(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				external) MISC(link is external)
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2 could allow an authenticated user to obtain sensitive information such as account lists due to improper access control. IBM X-Force ID: 120274.	2017-06-22	not yet calculated	CVE-2016-9982 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0 and 9.0 could allow an authenticated user to cause a denial of service to the MQXR channel when trace is enabled. IBM X-Force ID: 121155.	2017-06-21	not yet calculated	CVE-2017-1117 CONFIRM(link is external) BID(link is external) MISC(link is external)
inside_secure -- matrixssl	An exploitable heap buffer overflow vulnerability exists in the X509 certificate parsing functionality of Inside Secure MatrixSSL 3.8.7b. A specially crafted x509 certificate can cause a buffer overflow on the heap resulting in remote code execution. To trigger this vulnerability, a specially crafted x509 certificate must be presented to the vulnerable client or server application when initiating secure connection.	2017-06-22	not yet calculated	CVE-2017-2780 MISC(link is external)
inside_secure -- matrixssl	An exploitable heap buffer overflow vulnerability exists in the X509 certificate parsing functionality of InsideSecure MatrixSSL 3.8.7b. A specially crafted x509 certificate can cause a buffer overflow on the heap resulting in remote code execution. To trigger this vulnerability, a specially crafted x509 certificate must be presented to the vulnerable client or server	2017-06-22	not yet calculated	CVE-2017-2781 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application when initiating secure connection.			
inside_secure -- matrixssl	An integer overflow vulnerability exists in the X509 certificate parsing functionality of InsideSecure MatrixSSL 3.8.7b. A specially crafted x509 certificate can cause a length counter to overflow, leading to a controlled out of bounds copy operation. To trigger this vulnerability, a specially crafted x509 certificate must be presented to the vulnerable client or server application when initiating secure connection	2017-06-22	not yet calculated	CVE-2017-2782 MISC(link is external)
ipfire_project -- ipfire	IPFire 2.19 has a Remote Command Injection vulnerability in ids.cgi via the OINKCODE parameter, which is mishandled by a shell. This can be exploited directly by authenticated users, or through CSRF.	2017-06-19	not yet calculated	CVE-2017-9757 BID(link is external) MISC(link is external) EXPLOIT-DB(link is external)
irfan_skiljan -- irfan	An exploitable integer overflow vulnerability exists in the JPEG 2000 parser functionality of IrfanView 4.44. A specially crafted jpeg2000 image can cause an integer overflow leading to wrong memory allocation resulting in arbitrary code execution. Vulnerability can be triggered by viewing the image in via the application or by using thumbnailing feature of IrfanView.	2017-06-21	not yet calculated	CVE-2017-2813 BID(link is external) MISC(link is external)
jasper -- jasper	JasPer 2.0.12 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted image, related to the jp2_decode function in libjasper/jp2/jp2_dec.c.	2017-06-21	not yet calculated	CVE-2017-9782 MISC(link is external)
jetty -- jetty	Jetty through 9.4.x is prone to a timing channel in util/security/Password.java, which makes it easier for remote attackers	2017-06-16	not yet calculated	CVE-2017-9735 BID(link is external) MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to obtain access by observing elapsed times before rejection of incorrect passwords.			MISC(link is external)
lenovo -- lenovo_system_x_servers	In the IMM2 firmware of Lenovo System x servers, remote commands issued by LXCA or other utilities may be captured in the First Failure Data Capture (FFDC) service log if the service log is generated when that remote command is running. Captured command data may contain clear text login information. Authorized users that can capture and export FFDC service log data may have access to these remote commands.	2017-06-19	not yet calculated	CVE-2017-3744 CONFIRM(link is external)
lenovo -- multiple_products	If multiple users are concurrently logged into a single system where one user is sending a command via the Lenovo ToolsCenter Advanced Settings Utility (ASU), UpdateXpress System Pack Installer (UXSPI) or Dynamic System Analysis (DSA) to a second machine, the other users may be able to see the user ID and clear text password that were used to access the second machine during the time the command is processing.	2017-06-19	not yet calculated	CVE-2017-3743 CONFIRM(link is external)
lenovo -- xclarity_administrator	In Lenovo XClarity Administrator (LXCA) before 1.3.0, if service data is downloaded from LXCA, a non-administrative user may have access to password information for users that have previously authenticated to the LXCA's internal LDAP server, including administrative accounts and service accounts with administrative privileges. This is an issue only for users who have used local authentication with LXCA and not remote authentication against external LDAP or ADFS servers.	2017-06-19	not yet calculated	CVE-2017-3745 CONFIRM(link is external)
libmtp -- libmtp	An integer overflow vulnerability in ptp-pack.c (ptp_unpack_OPL function) of libmtp (version 1.1.12 and below) allows attackers to cause a denial of service (out-of-bounds memory access) or maybe remote code execution by inserting a	2017-06-23	not yet calculated	CVE-2017-9832 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mobile device into a personal computer through a USB cable.			
libmtp -- libmtp	An integer overflow vulnerability in the ptp_unpack_EOS_CustomFuncEx function of the ptp-pack.c file of libmtp (version 1.1.12 and below) allows attackers to cause a denial of service (out-of-bounds memory access) or maybe remote code execution by inserting a mobile device into a personal computer through a USB cable.	2017-06-23	not yet calculated	CVE-2017-9831 CONFIRM(link is external)
libnffi -- libnffi	libffi requests an executable stack allowing attackers to more easily trigger arbitrary code execution by overwriting the stack. Please note that libffi is used by a number of other libraries. This affects libffi version 3.2.1.	2017-06-19	not yet calculated	CVE-2017-1000376 CONFIRM(link is external) MISC(link is external)
libtiff -- libtiff	In LibTIFF 4.0.7, the TIFFReadDirEntryLong8Array function in libtiff/tif_dirread.c mishandles a malloc operation, which allows attackers to cause a denial of service (memory leak within the function _TIFFmalloc in tif_unix.c) via a crafted file.	2017-06-22	not yet calculated	CVE-2017-9815 MISC MISC(link is external) BID(link is external)
libtorrent -- libtorrent	The bdecode function in bdecode.cpp in libtorrent 1.1.3 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file.	2017-06-24	not yet calculated	CVE-2017-9847 CONFIRM(link is external)
linux -- linux_kernel	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).	2017-06-19	not yet calculated	CVE-2017-1000364 BID(link is external) CONFIRM(link is external) MISC(link is external) CONFIRM(link is external) CONFIRM(

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				link is external)
linux -- linux_kernel	The Linux Kernel running on AMD64 systems will sometimes map the contents of PIE executable, the heap or ld.so to where the stack is mapped allowing attackers to more easily manipulate the stack. Linux Kernel version 4.11.5 is affected.	2017-06-19	not yet calculated	CVE-2017-1000379 CONFIRM(link is external) MISC(link is external)
linux -- linux_kernel	The Linux Kernel imposes a size restriction on the arguments and environmental strings passed through RLIMIT_STACK/RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23.	2017-06-19	not yet calculated	CVE-2017-1000365 BID(link is external) CONFIRM(link is external) MISC(link is external)
linux -- linux_kernel	The offset2lib patch as used in the Linux Kernel contains a vulnerability that allows a PIE binary to be execve()'ed with 1GB of arguments or environmental strings then the stack occupies the address 0x80000000 and the PIE binary is mapped above 0x40000000 nullifying the protection of the offset2lib patch. This affects Linux Kernel version 4.11.5 and earlier. This is a different issue than CVE-2017-1000371. This issue appears to be limited to i386 based systems.	2017-06-19	not yet calculated	CVE-2017-1000370 BID(link is external) CONFIRM(link is external) MISC(link is external)
linux -- linux_kernel	An issue was discovered in the size of the default stack guard page on PAX Linux (originally from GRSecurity but shipped by other Linux vendors), specifically the default stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects PAX Linux Kernel versions as of June 19, 2017 (specific version information is not available at this time).	2017-06-19	not yet calculated	CVE-2017-1000377 BID(link is external) CONFIRM(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	The offset2lib patch as used by the Linux Kernel contains a vulnerability, if RLIMIT_STACK is set to RLIM_INFINITY and 1 Gigabyte of memory is allocated (the maximum under the 1/4 restriction) then the stack will be grown down to 0x80000000, and as the PIE binary is mapped above 0x80000000 the minimum distance between the end of the PIE binary's read-write segment and the start of the stack becomes small enough that the stack guard page can be jumped over by an attacker. This affects Linux Kernel version 4.11.5. This is a different issue than CVE-2017-1000370 and CVE-2017-1000365. This issue appears to be limited to i386 based systems.	2017-06-19	not yet calculated	CVE-2017-1000371 BID(link is external) CONFIRM(link is external) MISC(link is external)
mcafee -- data_loss_prevention_endpoint	Cross Site Scripting (XSS) in IMG Tags in the ePO extension in McAfee Data Loss Prevention Endpoint (DLP Endpoint) 10.0.x allows authenticated users to inject arbitrary web script or HTML via injecting malicious JavaScript into a user's browsing session.	2017-06-23	not yet calculated	CVE-2017-3948 CONFIRM(link is external)
microsoft -- windows	A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled.	2017-06-22	not yet calculated	CVE-2017-0176 BID(link is external) BID(link is external) MISC(link is external) MISC(link is external) CONFIRM(link is external)
milwaukee_tool -- one-key_android_mobile_app	The Milwaukee ONE-KEY Android mobile application uses bearer tokens with an expiration of one year. This bearer token, in combination with a user_id can be used to perform user actions.	2017-06-19	not yet calculated	CVE-2017-3215 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
milwaukee_tool -- one-key_android_mobile_app	The Milwaukee ONE-KEY Android mobile application stores the master token in plaintext in the apk binary.	2017-06-19	not yet calculated	CVE-2017-3214 MISC(link is external)
multiple_vendors -- wimax_routers	WiMAX routers based on the MediaTek SDK (libmtk) that use a custom httpd plugin are vulnerable to an authentication bypass allowing a remote, unauthenticated attacker to gain administrator access to the device by performing an administrator password change on the device via a crafted POST request.	2017-06-19	not yet calculated	CVE-2017-3216 MISC(link is external) CERT-VN MISC(link is external)
netbsd -- netbsd	NetBSD maps the run-time link-editor ld.so directly below the stack region, even if ASLR is enabled, this allows attackers to more easily manipulate memory leading to arbitrary code execution. This affects NetBSD 7.1 and possibly earlier versions.	2017-06-19	not yet calculated	CVE-2017-1000375 MISC(link is external)
netbsd -- netbsd	A flaw exists in NetBSD's implementation of the stack guard page that allows attackers to bypass it resulting in arbitrary code execution using certain setuid binaries. This affects NetBSD 7.1 and possibly earlier versions.	2017-06-19	not yet calculated	CVE-2017-1000374 BID(link is external) MISC(link is external)
netbsd -- netbsd	The NetBSD qsort() function is recursive, and not randomized, an attacker can construct a pathological input array of N elements that causes qsort() to deterministically recurse N/4 times. This allows attackers to consume arbitrary amounts of stack memory and manipulate stack memory to assist in arbitrary code execution attacks. This affects NetBSD 7.1 and possibly earlier versions.	2017-06-19	not yet calculated	CVE-2017-1000378 MISC MISC(link is external)
ocaml -- ocaml	Insufficient sanitisation in the OCaml compiler versions 4.04.0 and 4.04.1 allows external code to be executed with raised privilege in binaries marked as setuid, by setting the CAML_CPLUGINS, CAML_NATIVE_CPLUGINS, or	2017-06-23	not yet calculated	CVE-2017-9772 CONFIRM(link is external) CONFIRM(

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CAML_BYTE_CPLUGINS environment variable.			link is external)
openbsd_project -- openbsd	The OpenBSD qsort() function is recursive, and not randomized, an attacker can construct a pathological input array of N elements that causes qsort() to deterministically recurse N/4 times. This allows attackers to consume arbitrary amounts of stack memory and manipulate stack memory to assist in arbitrary code execution attacks. This affects OpenBSD 6.1 and possibly earlier versions.	2017-06-19	not yet calculated	CVE-2017-1000373 BID(link is external) MISC MISC(link is external)
openbsd_project -- openbsd	A flaw exists in OpenBSD's implementation of the stack guard page that allows attackers to bypass it resulting in arbitrary code execution using setuid binaries such as /usr/bin/at. This affects OpenBSD 6.1 and possibly earlier versions.	2017-06-19	not yet calculated	CVE-2017-1000372 BID(link is external) MISC MISC(link is external)
openwebif -- openwebif	An issue was discovered in the OpenWebif plugin through 1.2.4 for E2 open devices. The saveConfig function of "plugin/controllers/models/config.py" performs an eval() call on the contents of the "key" HTTP GET parameter. This allows an unauthenticated remote attacker to execute arbitrary Python code or OS commands via api/saveconfig.	2017-06-21	not yet calculated	CVE-2017-9807 BID(link is external) CONFIRM(link is external)
oracle -- sun_systems_products_suite	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in takeover of Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2017-06-22	not yet calculated	CVE-2017-3629 CONFIRM(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- sun_systems_products_suite	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2017-06-22	not yet calculated	CVE-2017-3631 CONFIRM(link is external) BID(link is external)
oracle -- sun_systems_products_suite	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2017-06-22	not yet calculated	CVE-2017-3630 CONFIRM(link is external) BID(link is external)
piwigo -- piwigo	Cross-site scripting (XSS) vulnerability in Piwigo 2.9.1 allows remote authenticated administrators to inject arbitrary web script or HTML via the virtual_name parameter	2017-06-24	not yet calculated	CVE-2017-9836 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to /admin.php (i.e., creating a virtual album).			
piwigo -- piwigo	The ws_session_logout function in Piwigo 2.9.1 and earlier does not properly delete user login cookies, which allows remote attackers to gain access via cookie reuse.	2017-06-24	not yet calculated	CVE-2017-9837 MISC(link is external)
poppler -- poppler	Stack buffer overflow in GfxState.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) via a crafted PDF document.	2017-06-22	not yet calculated	CVE-2017-9775 CONFIRM
poppler -- poppler	Integer overflow leading to Heap buffer overflow in JBIG2Stream.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.	2017-06-22	not yet calculated	CVE-2017-9776 CONFIRM
projectsend -- r754	install/make-config.php in ProjectSend r754 allows remote attackers to execute arbitrary PHP code via the dbprefix parameter, related to replacing TABLES_PREFIX in the configuration file.	2017-06-18	not yet calculated	CVE-2017-9741 MISC(link is external)
radare2 -- radare2	The cmd_info function in libr/core/cmd_info.c in radare2 1.5.0 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted binary file.	2017-06-19	not yet calculated	CVE-2017-9762 BID(link is external) CONFIRM(link is external)
radare2 -- radare2	The find_eoq function in libr/core/cmd.c in radare2 1.5.0 allows remote attackers to cause a denial of service (heap-based out-of-bounds read and application crash) via a crafted binary file.	2017-06-19	not yet calculated	CVE-2017-9761 BID(link is external) CONFIRM(link is external) CONFIRM(

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				link is external)
radare2 -- radare2	The grub_ext2_read_block function in fs/ext2.c in GNU GRUB before 2013-11-12, as used in shlr/grub/fs/ext2.c in radare2 1.5.0, allows remote attackers to cause a denial of service (excessive stack use and application crash) via a crafted binary file, related to use of a variable-size stack array.	2017-06-19	not yet calculated	CVE-2017-9763 CONFIRM BID(link is external) CONFIRM(link is external) CONFIRM(link is external)
redgate -- sql_monitor	In Redgate SQL Monitor before 3.10 and 4.x before 4.2, a remote attacker can gain unauthenticated access to the Base Monitor, resulting in the ability to execute arbitrary SQL commands on any monitored Microsoft SQL Server machines. If the Base Monitor is connecting to these machines using an account with SQL admin privileges, then code execution on the operating system can result in full system compromise (if Microsoft SQL Server is running with local administrator privileges).	2017-06-22	not yet calculated	CVE-2015-9098 CONFIRM(link is external)
samsung -- magician	Samsung Magician 5.0 fails to validate TLS certificates for HTTPS software update traffic. Prior to version 5.0, Samsung Magician uses HTTP for software updates.	2017-06-21	not yet calculated	CVE-2017-3218 BID(link is external) CERT-VN
sitecore -- sitecore.net	Sitecore.NET 7.1 through 7.2 has a Cross Site Scripting Vulnerability via the searchStr parameter to the /Search-Results URI.	2017-06-23	not yet calculated	CVE-2017-9356 MISC
sophos -- anti-virus_threat_detection_engine	A VMSF_DELTA memory corruption was discovered in unrar before 5.5.5, as used in Sophos Anti-Virus Threat Detection Engine before 3.37.2 and other products, that can lead to arbitrary code execution. An integer overflow can be caused in DataSize+CurChannel. The result is a	2017-06-22	not yet calculated	CVE-2012-6706 MISC(link is external) MISC(link is external) MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	negative value of the "DestPos" variable, which allows the attacker to write out of bounds when setting Mem[DestPos].			MISC(link is external) MISC(link is external) MISC(link is external)
trihedral_engineering -- vtscada	An Information Exposure issue was discovered in Trihedral VTScada Versions prior to 11.2.26. Some files are exposed within the web server application to unauthenticated users. These files may contain sensitive configuration information.	2017-06-21	not yet calculated	CVE-2017-6045 BID(link is external) MISC
trihedral_engineering -- vtscada	A Cross-Site Scripting issue was discovered in Trihedral VTScada Versions prior to 11.2.26. A cross-site scripting vulnerability may allow JavaScript code supplied by the attacker to execute within the user's browser.	2017-06-21	not yet calculated	CVE-2017-6053 BID(link is external) MISC
trihedral_engineering -- vtscada	A Resource Consumption issue was discovered in Trihedral VTScada Versions prior to 11.2.26. The client does not properly validate the input or limit the amount of resources that are utilized by an attacker, which can be used to consume more resources than are available.	2017-06-21	not yet calculated	CVE-2017-6043 BID(link is external) MISC
vivotek -- network_cameras	'/cgi-bin/admin/testserver.cgi' of the web service in most of the VIVOTEK Network Cameras is vulnerable to shell command injection, which allows remote attackers to execute any shell command as root via a crafted HTTP request. This vulnerability is already verified on VIVOTEK Network Camera IB8369/FD8164/FD816BA; most others have similar firmware that may be affected. An attack uses shell metacharacters in the senderemail parameter.	2017-06-23	not yet calculated	CVE-2017-9828 MISC(link is external)
vivotek -- network_cameras	'/cgi-bin/admin/downloadMedias.cgi' of the web service in most of the VIVOTEK Network Cameras is vulnerable, which allows remote attackers to read any file on	2017-06-23	not yet calculated	CVE-2017-9829

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the camera's Linux filesystem via a crafted HTTP request containing ".." sequences. This vulnerability is already verified on VIVOTEK Network Camera IB8369/FD8164/FD816BA; most others have similar firmware that may be affected.			MISC(link is external)
websitebaker_org -- websitebaker	install\save.php in WebsiteBaker v2.10.0 allows remote attackers to execute arbitrary PHP code via the database_username parameter.	2017-06-21	not yet calculated	CVE-2017-9771 MISC(link is external)
winmail -- winmail_server	Winmail Server 6.1 allows remote code execution by authenticated users who leverage directory traversal in a netdisk.php move_folder_file call to move a .php file from the FTP folder into a web folder.	2017-06-24	not yet calculated	CVE-2017-9846 MISC(link is external) MISC(link is external)
wireshark -- wireshark	In Wireshark 2.2.7, PROFINET IO data with a high recursion depth allows remote attackers to cause a denial of service (stack exhaustion) in the dissect_IODWriteReq function in plugins/profinet/packet-dcerpc-pn-io.c.	2017-06-21	not yet calculated	CVE-2017-9766 BID(link is external) CONFIRM CONFIRM