-	National	Critica	l Informat	ion Infra	astructu	re Pro	tection Ce	entre	
Judiere J			<i>CVE Re</i> 16-31 Ju	-	5			Vol.	03 No. 13
Vulnerability Type(s)	Publish Date	CVSS	Descriptio	n			Patch		NCIIPC ID
			Appli	cation(A)				
Apache									
Archiva Apache Archiva personal or ente		-		-	ware tha	t helps	taking care	of you	ir own
Cross Site Scripting	28/07/2016	3.5	Cross-site vulnerabi 1.3.9 and authentic inject arbi HTML via connector paramete admin/ad mmit.activ	scripting lity in Ap earlier al ated adm trary we the :.sourceR r to dProxyC on.	ache Arc lows rem inistrato b script o epoId onnector	note rs to or _co	NA		A-APA- ARCHI- 50816/01
Http Server The Apache HTT modern operation	-	-		-	naintain	an oper	n-source HT	TP ser	rver for
NA	18/07/2016	5.1	The Apach through 2 3875 sect therefore application of untrust HTTP_PRO variable, w remote at application traffic to a server via header in an "httpo: vendor sta has been a CVE-2016	ne HTTP .4.23 foll ion 4.1.13 does not ns from t ed client DXY envi vhich mi tackers te n's outbo n arbitra a crafteo an HTTP cy" issue. ates "This assigned	ows RFC 8 and protect the prese data in t ronment ght allow o redirec ound HTT ury proxy l Proxy request, NOTE: th s mitigati the ident	nce he t an TP aka he ion ifier	https://ww pache.org/ rity/asf- httpoxy- response.t	/secu	A-APA- HTTP - 50816/02
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Tomcat				words, thi vulnerabi Referenc	lity.							
Apache Tomco Foundation (A	· · ·	eferred to	o as Tom	icat, is an o	pen-sour	ce web se	rver de	evel	loped by	the Ap	ach	eSoftwar
NA	· ·	/2016	5.1	Apache To when the follows RI and there applicatio of untrust HTTP_PRO variable, w remote at applicatio traffic to a server via header in an "httpox vendor sta planned fo Tomcat, th 5388"; in not a CVE Referenc	CGI Servi FC 3875 s fore does ns from t ed client DXY envi which mig tackers to n's outbo in arbitra a crafted an HTTP ky" issue. ates "A m or future racked as other wo ID for a v	et is enal section 4. not prot he prese data in the conment of allow oredirec ound HTT ry proxy Proxy Proxy Proxy request, NOTE: the itigation releases CVE-202 rds, this vulnerabi	bled, 1.18 nce he t an TP aka he is of 16- is lity.	pa rit ht	tps://ww iche.org/ cy/asf- tpoxy- sponse.t	'secu	TC	APA- MCA 816/03
Apple												
Safari Safari is a wel	b browser	develope	ed by App	ple based of	n the Wel	oKit engi	ne.					
NĂ	1	/2016	5.8	Safari in A allows rer spoof the HTTP resp redirectio port numl Referenc	apple iOS note atta displayed oonse spe n to an ir oer.	before 9 ckers to l URL via ecifying walid TC	.3.3 1 an P	t.a	tps://su pple.con 206902		SA	APP- FAR 816/04
Safari;Webk Safari is a wel browser engir	b browser	develope	ed by App	ple based of	n the Wel	oKit engii	ne; Wel	bKi	t is an op	oen soi	ırce	web
NA		/2016		WebKit in Apple iOS before 9.3.3https://suand Safari before 9.1.2t.apple.cormishandles about: URLs, whichT206902allows remote attackers to						SA	APP- FAR 816/05	
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7		7-8	8-9		9-10

			bypass the Same Origin Policy via a crafted web site. Reference: CVE-2016-4590		
Webkit WebKit is an one	n agurag uich h	NO11100M 0	ngina		
<u>WebKit is an ope</u> Denial of Service	21/07/2016	7.1	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to cause a denial of service (memory consumption) via a crafted web site. Reference: CVE-2016-4592	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/06
NA	21/07/2016	7.8	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 mishandles the location variable, which allows remote attackers to access the local filesystem via unspecified vectors. Reference: CVE-2016-4591	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/07
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	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- 4622, CVE-2016-4623, and CVE- 2016-4624. Reference: CVE-2016-4589	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/08
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	WebKit in Apple 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. Reference: CVE-2016-4588	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/09
Overflow; Gain Info	21/07/2016	4.3	WebKit in Apple iOS before 9.3.3 and tvOS before 9.2.2 allows remote attackers to obtain sensitive information from uninitialized process memory	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/10

CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
---------------------	---------	-----	-----	-----	-----	-----	-----	-----	------

			via a crafted web site. Reference: CVE-2016-4587		
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	WebKit in Apple 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. Reference: CVE-2016-4586	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/11
Cross Site Scripting	21/07/2016	4.3	Cross-site scripting (XSS) vulnerability in the WebKit Page Loading implementation in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to inject arbitrary web script or HTML via an HTTP response specifying redirection that is mishandled by Safari. Reference: CVE-2016-4585	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/12
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	The WebKit Page Loading implementation 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. Reference: CVE-2016-4584	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/13
Bypass	21/07/2016	4.3	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to bypass the Same Origin Policy and obtain image date from an unintended web site via a timing attack involving an SVG document. Reference: CVE-2016-4583	https://suppor t.apple.com/H T206905	A-APP- WEBKI 50816/14

Ehealth

eHealth is a relatively recent term for healthcare practice supported by electronic processes and communication.

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Denial of Service; Execute Code	25/07/2016	9	CA eHealth 6.3.2.13 al authentica denial of s execute ar unspecifie Reference	lows rem ted users ervice or bitrary co d vectors	ote s to cause possibly ommand	e a , s via	http://ww .com/us/s rt/ca-supp online/pro content/ro mended- reading/s ty notices/ca 60721-01 security- notice-for ehealth.as	suppo port- oduct ecom ecuri a201 - -ca-	A-CA- EHEAL 50816/15
Denial of Service; Execute Code	25/07/2016	9	CA eHealth authentica denial of s execute ar unspecifie Reference	ted users ervice or bitrary co d vectors	s to cause possibly ommand	e a , s via	http://ww .com/us/s rt/ca-supp online/pro- - content/r mended- reading/s ty- notices/ca 60721-01 security- notice-for ehealth.as	vw.ca suppo port- oduct ecom ecuri a201 - -ca-	A-CA- EHEAL 50816/16
Ec-cube								<u>F</u>	
Coupon Plugin									
JC Coupon is a W		_				-			
Execute Code; SQL Injection	31/07/2016	7.5	SQL injecti Seed Coup for EC-CUI attackers t SQL comm vectors. Reference	on plugir 3E allows to execute ands via	n before remote e arbitrat unspecif	1.6 ry fied	http://ww - cube.net/j ucts/detai ?product_ 93	prod il.php	A-EC COUPO 50816/17
Golang			Reference		10 105	,			
GO Go is an open so software.	urce programm	ing lang	uage that m	akes it e	asy to bu	ild simp	ole, reliable	, and ej	fficient
NA	18/07/2016	5.1	The net/h through 1		-		https://bu a.redhat.co	-	A-GOL-GO 50816/18
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			implementation in Blink, as used in Google Chrome before 52.0.2743.82, does not apply http :80 policies to https :443 URLs and does not apply ws :80 policies to wss :443 URLs, which makes it easier for remote	update.html	
			URLs and does not apply ws :80 policies to wss :443 URLs, which		
			52.0.2743.82, does not apply	blogspot.com/ 2016/07/stabl e-channel- update.html	50816/19
NA	23/07/2016	4.3	The CSPSource::schemeMatches function in WebKit/Source/core/frame/cs	http://googlec hromereleases.	A-GOO- CHROM
Chrome Google Chrome			er developed by Google.		
Google			Reference: CVE-2016-5386		
			variable, which might allow remote attackers to redirect a CGI application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue.		
			address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect CGI applications from the presence of untrusted client data in the HTTP_PROXY environment	how_bug.cgi?id =1353798	

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1 0	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	--------------	--

			denial of service or possibly have unspecified other impact via vectors related to script deletion.		
Bypass	23/07/2016	4.3	Reference: CVE-2016-5136 WebKit/Source/core/html/pars er/HTMLPreloadScanner.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not consider referrer-policy information inside an HTML document during a preload request, which allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a crafted web site, as demonstrated by a "Content-Security-Policy: referrer origin-when-cross- origin" header that overrides a " <meta <br="" name="referrer"/> content='no-referrer'>" element. Reference: CVE-2016-5135	https://crbug.c om/605451	A-GOO- CHROM 50816/21
NA	23/07/2016	4.3	net/proxy/proxy_service.cc in the Proxy Auto-Config (PAC) feature in Google Chrome before 52.0.2743.82 does not ensure that URL information is restricted to a scheme, host, and port, which allows remote attackers to discover credentials by operating a server with a PAC script, a related issue to CVE-2016-3763. Reference: CVE-2016-5134	http://googlec hromereleases. blogspot.com/ 2016/07/stabl e-channel- update.html	A-GOO- CHROM 50816/22
NA	23/07/2016	4.3	Google Chrome before 52.0.2743.82 mishandles origin information during proxy authentication, which allows man-in-the-middle attackers to spoof a proxy-authentication login prompt or trigger incorrect credential storage by	http://googlec hromereleases. blogspot.com/ 2016/07/stabl e-channel- update.html	A-GOO- CHROM 50816/23

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

			modifying the client-server data stream. Reference: CVE-2016-5133		
Bypass	23/07/2016	6.8	The Service Workers subsystem in Google Chrome before 52.0.2743.82 does not properly implement the Secure Contexts specification during decisions about whether to control a subframe, which allows remote attackers to bypass the Same Origin Policy via an https IFRAME element inside an http IFRAME element. Reference: CVE-2016-5132	https://codere view.chromiu m.org/208249 3002/	A-GOO- CHROM 50816/24
NA	23/07/2016	4.3	content/renderer/history_contr oller.cc in Google Chrome before 52.0.2743.82 does not properly restrict multiple uses of a JavaScript forward method, which allows remote attackers to spoof the URL display via a crafted web site. Reference: CVE-2016-5130	https://crbug.c om/623319	A-GOO- CHROM 50816/25
Denial of Service	23/07/2016	6.8	Use-after-free vulnerability in WebKit/Source/core/editing/Vi sibleUnits.cpp in Blink, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code involving an @import at-rule in a Cascading Style Sheets (CSS) token sequence in conjunction with a rel=import attribute of a LINK element. Reference: CVE-2016-5127	https://codere view.chromiu m.org/209163 3002	A-GOO- CHROM 50816/26
Denial of Service; Overflow	31/07/2016	6.8	Integer overflow in the kbasep_vinstr_attach_client function in midgard/mali_kbase_vinstr.c in	https://bugs.c hromium.org/ p/chromium/i ssues/detail?id	A-GOO- CHROM 50816/27

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

			Google Chrome before 52.0.2743.85 allows remote attackers to cause a denial of service (heap-based buffer overflow and use-after-free) by leveraging an unrestricted multiplication. Reference: CVE-2016-5138	=631752&desc =2	
Chrome;V8	<u> </u>				
0	· ·		er developed by Google; The V8 Java		n open source
			mium Project for the Google Chrom		1.000
Denial of Service; Overflow Memory Corruption	23/07/2016	6.8	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. Reference: CVE-2016-5129	https://crbug.c om/620553	A-GOO- CHROM 50816/28
Bypass	23/07/2016	6.8	objects.cc in Google V8 before 5.2.361.27, as used in Google Chrome before 52.0.2743.82, does not prevent API interceptors from modifying a store target without setting a property, which allows remote attackers to bypass the Same Origin Policy via a crafted web site. Reference: CVE-2016-5128	https://crbug.c om/619166	A-GOO- CHROM 50816/29
Google;Xmlsof	t			I	
Chrome/Libxm	1 <mark>12</mark> is a freeware we	eb brows	er developed by Google; libxml2 is a	software library fo	or parsing
Denial of Service	23/07/2016	6.8	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have	https://crbug.c om/623378	A-GOO- CHROM 50816/30
CV Scoring	0-1 1-2	2-3	3-4 4-5 5-6 6-7	7-8 8-9	9-10

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

			unerpacified other impact via		
			unspecified other impact via vectors related to the XPointer		
			range-to function.		
Lau Duaia at			Reference: CVE-2016-5131		
Icu Project					
	Components Fo				
			ICU) is an open source project of ma malization, and software globalizati		va libraries
Denial of	25/07/2016	7.5	The	011.	A-ICU-
Service;	25/07/2010	7.0	uloc_acceptLanguageFromHTTP		INTER
Overflow			function in common/uloc.cpp in		50816/31
			International Components for		00010/01
			Unicode (ICU) through 57.1 for		
			C/C++ does not ensure that		
			there is a '\0' character at the		
			end of a certain temporary		
			array, which allows remote		
			attackers to cause a denial of		
			service (out-of-bounds read) or		
			possibly have unspecified other		
			impact via a call with a long		
			httpAcceptLanguage argument.		
			Reference: CVE-2016-6293		
Intel	<u> </u>				
Intel Crosswalk					
Crosswalk	 	built on		ends the web platfo	orm with new
Crosswalk	 TML5 runtime,	built on	Reference: CVE-2016-6293	ends the web platfo	orm with new
<mark>Crosswalk</mark> Crosswalk is a H	<i>ITML5 runtime,</i> 31/07/2016	built on	Reference: CVE-2016-6293	ends the web platfo	orm with new A-INT-
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which exte		
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 <i>open source foundations, which external</i> Intel Crosswalk before	https://blogs.i	A-INT-
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before	https://blogs.i ntel.com/evan	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before	https://blogs.i ntel.com/evan gelists/2016/0	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting, which makes it easier for man-	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting,	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting, which makes it easier for man- in-the-middle attackers to spoof	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting, which makes it easier for man- in-the-middle attackers to spoof SSL servers and obtain sensitive	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting, which makes it easier for man- in-the-middle attackers to spoof SSL servers and obtain sensitive information via a crafted certificate.	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
<mark>Crosswalk</mark> Crosswalk is a H capabilities.			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting, which makes it easier for man- in-the-middle attackers to spoof SSL servers and obtain sensitive information via a crafted	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security-	A-INT- CROSS
Crosswalk Crosswalk is a H capabilities. NA			Reference: CVE-2016-6293 open source foundations, which external Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting, which makes it easier for man- in-the-middle attackers to spoof SSL servers and obtain sensitive information via a crafted certificate.	https://blogs.i ntel.com/evan gelists/2016/0 7/28/crosswal k-security- vulnerability/	A-INT- CROSS 50816/32

Fusioncapital Opics Plus

MISYS Fusion Capital Opics is the .NET service-oriented Treasury and Capital Markets solution with unsurpassed STP and back-office capabilities.

unsurpassed ST			e capabili	ities.								
NA	19/07	/2016		Misys Fus does not v certificate which allo middle at sensitive crafted ce Referenc	verify X.5 es from S ows man- tackers to information rtificate.	09 SL server in-the- o obtain on via a	S,	http://www.kb .cert.org/vuls/i d/682704			FU	MIS- JSIO 1816/33
NA	19/07	/2016		Misys Fus allows rei users to g man-in-th modifies t paramete Referenc	mote auth ain privil ne-middle the xmlM r.	nenticate eges via attack tl essageOu	d a hat ıt	.ce	tp://ww ert.org/v ′682704		FU	MIS- JSIO 9816/34
Execute Code; SQL Injection	19/07	/2016		Multiple S vulnerabil FusionCap remote au execute ar command Branch pa Referenc	ities in M bital Opic thenticat bitrary S s via the rameter.	isys s Plus alle ed users QL (1) ID or	to (2)	.ce	tp://ww ert.org/v ′682704		FU	MIS- JSIO 9816/35
Objective Syst	ems		·	<u>Merer ence</u>		10 303	5					
Asn1c ASN1C ASN.1 Co	ompiler (anslates	ASN.1	and	d/or XML	schen	na ((XSD)
Denial of Service; Execute Code; Overflow		/2016	10	Integer overflow in the rtxMemHeapAlloc function in asn1rt_a.lib in Objective Systems ASN1C for C/C++ before 7.0.2 allows context-dependent attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow), on a system running an application compiled by ASN1C, via crafted ASN.1 data. Reference: CVE-2016-5080				NA	A		AS	OBJ- SN1C 1816/36
Oracle												
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	,	7-8	8-9		9-10

Agile Product Lifecycle Management Framework With Oracle's easy-to-use product lifecycle management solutions, you can accelerate time-to-market, reduce costs, and increase profitability.

reduce costs, an			ability.									
NA	21/07	/2016	3.5	Unspecifie Oracle Ag Oracle Su Suite 9.3.4 remote au affect con related to Attachme vulnerabi 3537. Referenc	ile PLM c pply Chai 4 and 9.3. tthenticat fidentiali File Fold nt, a diffe lity than	omponen n Produc 5 allows ced users ty via vec ers / rent CVE-201	nt in cts s to ctors 6-	ac et y- ad 12	tp://ww le.com/t work/se lvisory/c 016- 381720.h	echn curit cpuju	AG	DRA- ILE 816/37
Communicatio <i>NA</i>	ons Eagl	e Applie	cation P	rocessor								
NA	21/07	/2016		Unspecifie Oracle Con Applicatio componen Communio 16.0 allow authentica confidenti vectors re Reference	nmunica n Process at in Orac cations A rs remote ated users ality and lated to A	tions EA(sor le pplicatio s to affect integrity .PPL.	GLE ns t via	ac et y- ad 12	tp://ww le.com/t work/se lvisory/c 016- 381720.h	echn curit cpuju	CO	DRA- MMU 816/38
Communicatio			Server									
The Oracle Com for delivering se					ides a hig	hly scala	ble, rel	liab	ole, and a	vailab	le pl	atform
NA NA		/2016	5	Unspecific Oracle Co Messaging Oracle Co Application allows rem affect con related to	mmunica g Server (mmunica ons 6.3, 7 note atta fidentiali Multiple	tions compone tions 0, and 8. ckers to ty via veo xor.	nt in 0 ctors	ac et y- ad 12	tp://ww le.com/t work/se lvisory/c 016- 381720.h	echn curit cpuju	CO	DRA- MMU 816/39
Glassfish Serv Oracle GlassFish 6 specification.		is the wo	orld's firs	Reference: CVE-2016-5455 rst implementation of the Java Platfo				rm,	Enterpr	ise Edi	tion	(Java EE)
NA	21/07	/2016	5	Unspecifie Oracle Gla		•	the		tp://ww le.com/t			DRA- ASS
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7		7-8	8-9		9-10

<mark>Mysql</mark> MySQL is an ope NA	en-source relat		Reference: CVE-2016-5477 <i>abase management system (RDBMS)</i> Unspecified vulnerability in		
MySQL is an ope					
NA	21/07/2016	5 4.3	Unspecified vulnerability in	•	
			Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows remote attackers to affect confidentiality via vectors related to Server: Connection. Reference: CVE-2016-5444	http://www.or acle.com/techn etwork/securit y- advisory/cpuju l2016- 2881720.html	A-ORA- MYSQL 50816/41
NA	21/07/2016	5 1.2	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows local users to affect availability via vectors related to Server: Connection. Reference: CVE-2016-5443	http://www.or acle.com/techn etwork/securit y- advisory/cpuju l2016- 2881720.html	A-ORA- MYSQL 50816/42
NA	21/07/2016	5 4	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Encryption. Reference: CVE-2016-5442	http://www.or acle.com/techn etwork/securit y- advisory/cpuju l2016- 2881720.html	A-ORA- MYSQL 50816/43
NA	21/07/2016	5 <u>4</u>	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Replication. Reference: CVE-2016-5441	http://www.or acle.com/techn etwork/securit y- advisory/cpuju l2016- 2881720.html	A-ORA- MYSQL 50816/44
NA	21/07/2016	5 4	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows remote administrators to affect availability via vectors related	http://www.or acle.com/techn etwork/securit y- advisory/cpuju l2016-	A-ORA- MYSQL 50816/45

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	------------	-----	-----	-----	------	--

				to Server: Referenc		016-544	0	2881720.1	ntml	
NA	21/07	/2016	4	Unspecifie Oracle My and 5.7.12 remote ad availabilit to Server: Referenc	ed vulner SQL 5.6.3 2 and ear 1 ministra y via vect Privilege	ability in 80 and ea ier allow tors to af cors relat es.	nrlier vs ffect ced	http://ww acle.com/r etwork/se y- advisory/r l2016- 2881720.l	techn ecurit cpuju	A-ORA- MYSQL 50816/46
NA	21/07	/2016	4	Unspecifie Oracle My allows rer affect avai related to Referenc	SQL 5.7.2 note adm lability v Server: I	2 and ea inistrato ia vector og.	arlier ors to s	http://ww acle.com/r etwork/se y- advisory/e l2016- 2881720.l	techn ecurit cpuju	A-ORA- MYSQL 50816/47
NA	21/07	/2016	4	Unspecifie Oracle My allows rer affect avai related to Referenc	SQL 5.7.2 note adm lability v Server: I	2 and ea inistrato ia vector nnoDB.	arlier ors to s	http://ww acle.com/ etwork/se y- advisory/ l2016- 2881720.l	techn ecurit cpuju	A-ORA- MYSQL 50816/48
Peoplesoft E PeopleTools is Corporation. 2 and various of	s the propr The People	rietary so Tools co	oftware and the of a second se							
NA	21/07		7.2	Unspecifie PeopleSof PeopleTod Oracle Peo and 8.55 a affect cont and availa related to Referenc	t Enterpr ols compo opleSoft l allows loc fidentiali bility via Install ar	ise onent in Products al users ty, integr vectors ad Packag	8.54 to 'ity, ging.	http://ww acle.com/ etwork/se y- advisory/ l2016- 2881720.l	techn ecurit cpuju	A-ORA- PEOPL 50816/49
NA	21/07	/2016	7.1	Unspecifie PeopleSof PeopleToo Oracle Peo and 8.55 a attackers confident	t Enterpr ols compo opleSoft l illows rep to affect	rise onent in Products note		http://ww acle.com/ etwork/se y- advisory/ l2016- 2881720.l	techn ecurit cpuju	A-ORA- PEOPL 50816/50
CV Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

				related to Referenc			-				
NA		7/2016		Unspecifie PeopleSof PeopleToo Oracle Peo 8.53, 8.54 remote at confident vectors re Processor Referenc	t Enterpr ols comp opleSoft 1 , and 8.5 tackers to iality and lated to 1	rise onent in Products 5 allows 5 affect integrity Panel	y via	acl etv y- ad 120	tp://ww le.com/t work/se visory/c 016- 81720.h	echn curit cpuju	A-ORA- PEOPL 50816/51
Peoplesoft E					nchaoina		aantu		monding	inform	action for
PeopleSoft eP future analysi		nt neips e	enjorce co	ontract pu	rcnasing	as well as	scaptu	ire s	spenaing	Injorn	iation for
NA		7/2016		Unspecific PeopleSof componen PeopleSof allows ren users to a and integn related to Referenc	ft Enterpo nt in Orac ft Produc note auth ffect conf rity via ve eProcure	rise FSCM cle ts 9.1 and nenticate fidentialit ectors ement.	1 1 9.2 d ty	acle etw y- adv 202	p://www e.com/te vork/sec visory/cj 16- 31720.ht	echn curit pujul	A-ORA- PEOPL 50816/52
Retail Integr	ation Bus	S		<u>Merer ene</u>		010 510					
Oracle Retail	Integratio	n Bus (R									
guaranteed se		-				-				retry, t	he ability to
fix and retry r											A OD 4
NA		7/2016		Unspecific Oracle Re componen Applicatio 14.0, 14.1 remote au affect con and availa related to Referenc	tail Integ nt in Orac ons 13.0, , and 15.0 , thentica fidentiali ability via Install.	ration Bu le Retail 13.1, 13.2) allows ted users ty, integr vectors	is 2, ; to ; ity,	acle etw y- adv 202	p://www e.com/te vork/sec visory/cj 16- 31720.ht	echn curit pujul	A-ORA- RETAI 50816/53
Retail Servic The Retail Ser and provides	vice Back	bone (RS		•	-	s the Ora	cle Ret	ail I	Enterpris	se SOA	Architecture
NA		/2016	8	Unspecifie Oracle Re	ed vulner				p://www e.com/te		A-ORA- RETAI
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7		7-8	8-9	9-10

	•										
The Siebel Cor	re framework cons rkflow policies en 21/07/2016	sists of Se	-	nd Siebel d vulner e - Serve k compo bel CRM 2015, an note atta identiali lated to S ulnerabi	Tools. ability in r nent in 8.1.1, 8.2 d IP2016 ckers to ty via Services, a lity than	the .2, 5	htt acle etw y- adv 202	o://ww e.com/t vork/see	w.or echn curit pujul	e, Task A-OR SIEBE 50810	4- :
JA Siebel Core-s	21/07/2016	4.3 rk	Unspecifie Siebel Core Componen Oracle Sieh IP2014, IP allows rem affect integ related to i Reference	e - Comm ts compo oel CRM 8 2015, an tote attac grity via v Help.	on onent in 3.1.1, 8.2. d IP2016 ckers to vectors	2,	acle etw y- adv 202	p://ww e.com/t vork/sec isory/c 6- 31720.h	echn curit pujul	A-OR SIEBE 50810	
VA Siebel Core-c	21/07/2016	9 9 nents	component Applicatio 15.0 allow authentica confidenti availability to Install. Reference Unspecifie Oracle Ret component Applicatio 15.0 allow authentica confidenti availability to RSB Ken	ns 14.0, s remote ality, inte y via vect e: CVE-2 d vulner ail Servie it in Orac ns 14.0, s remote ality, inte y via vect rnel.	14.1, and s to affece egrity, an cors relat 016-547 ability in ce Backbo le Retail 14.1, and s to affece egrity, an cors relat	t ed 5 the one t d ed	y- adv 202 288 http aclo etw y- adv 202	31720.h p://ww e.com/t vork/see	pujul tml w.or echn curit pujul	50810 A-OR RETA 50810	A- I

CV Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Scale										

				Referenc	e: CVE-2	016-546	6					
	21/07	/2016	4	Unspecifie Siebel Cor Framewo Oracle Sie IP2014, IF allows ren to affect c vectors re Referenc	re - Serve rk compo- bel CRM 22015, an note adm onfidenti lated to V	r onent in 8.1.1, 8.2 d IP2010 inistrato ality via Workspa	2.2, 6 ors ces.	acl etv y- ad ⁻ 20	p://www e.com/te work/sec visory/cp 16- 81720.ht	echn aurit oujul	SIE	0RA- BE 316/58
NA	21/07		4	Unspecifie Siebel Cor Framewo Oracle Sie IP2014, IF allows ren users to a via vector Manager. Referenc	e - Serve rk compo- bel CRM 22015, an note auth ffect conf s related e: CVE-2	r onent in 8.1.1, 8.2 d IP2010 nenticate identiali to Objec 016-546	2.2, 6 d ty t	acl etv y- ad ¹ 20 28	p://www e.com/te work/sec visory/cp 16- 81720.ht	echn curit cujul cml	SIE 508	0RA- BE 316/59
NA	21/07	/2016	4.3	Unspecifie Siebel Cor Framewor Oracle Sie IP2014, IF allows ren affect con vectors red different v CVE-2016 5466. Referenc	re - Serve rk compo- bel CRM 22015, an note atta fidentiali lated to S vulnerabi 5-3450 an	r onent in 8.1.1, 8.2 d IP2010 ckers to ty via Services, lity than d CVE-20	2.2, 6 a 016-	acl etv y- ad ¹ 20	e.com/te work/sec visory/cp 16- 81720.ht	echn surit pujul	SIE	0RA- BE 316/60
NA	21/07	/2016		Unspecifie Siebel Cor componen CRM 8.1.1 IP2015, ar remote au affect conf related to Reference	d vulnera e - Serven t in Orac , 8.2.2, IP nd IP2016 thenticat fidentialit Services.	ability in Framew le Siebel 2014, 6 allows ed users ty via vec	the vork to ctors	acl etv y- ad ¹ 20	e.com/te work/sec visory/cp 16- 81720.ht	echn urit oujul	SIE	DRA- BE 316/61
Siebel Ui Fran Siebel Open UI		n archite						er in	terface ti	hat yoı	ır en	iterprise
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9		9-10

uses to display b	-		-								
NA	21/07/20	16	5.5	Unspecifie Siebel UI F componen CRM 8.1.1, IP2015, an remote au affect conf integrity v EAI, a diffe than CVE-2 Reference	ramewo t in Orac 8.2.2, IP d IP2016 thenticat identialit ia vector erent vulu 2016-54	rk le Siebel 2014, 5 allows ed users cy and s related herability 51.	to to 7	le.c orl adv 01	p://ww com/tec x/securi visory/c 6- 81720.h	hnetw ty- pujul2	A-ORA- SIEBE 50816/62
Siebel Ui Fram	ework										
Siebel Open UI i	-				use to cu	stomize t	he use	er in	terface t	that you	r enterprise
<u>uses to display b</u> NA	21/07/20	-	<u>njorma</u> 3.5	Unspecifie Siebel UI F componen CRM 8.1.1,	ramewo t in Orac 8.2.2, IP	rk le Siebel 2014,	the	le.c orl adv	p://ww com/tec k/securi visory/c	hnetw ty-	A-ORA- SIEBE 50816/63
				IP2015, an remote au affect integ related to different v CVE-2016 Reference	thenticat grity via SWSE Se ulnerabi -5463.	ed users vectors rver, a lity than		01 28	6- 81720.h	tml	
NA	21/07/20		3.5	Unspecifie Siebel UI F componen CRM 8.1.1, IP2015, an remote au affect integ related to different v CVE-2016 Reference	ramewo t in Orac 8.2.2, IP d IP2016 thenticat grity via SWSE Se ulnerabi -5464. e: CVE-20	rk le Siebel 2014, 6 allows ed users vectors rver, a lity than 016-546	to 3	le.c orł adv 010 283	81720.h	hnetw ty- pujul2 tml	A-ORA- SIEBE 50816/64
NA	21/07/20	16	5.5	Unspecifie Siebel UI F componen CRM 8.1.1, IP2015, an remote au	ramewo t in Orac 8.2.2, IP d IP2016	rk le Siebel 2014, 5 allows		le.c orl adv 01	p://ww com/tec c/securi visory/c 6- 81720.h	hnetw ty- pujul2	A-ORA- SIEBE 50816/65
CV Scoring	0-1 1	-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-1 0

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

				affect conf integrity v EAI, a diffe than CVE- Reference	via vector erent vuli 2016-54	s related nerability 68.	y				
NA	21/07	7/2016	4.3	Unspecifie Siebel UI F componen CRM 8.1.1 IP2015, ar remote att integrity v UIF Open Reference	Framewo at in Orac , 8.2.2, IP ad IP2010 tackers to ria vector UI.	rk le Siebel 2014, 6 allows 9 affect 5 related	to	le. or ad 01	tp://www com/tech k/securit visory/cj 6- 81720.ht	nnetw ty- pujul2	A-ORA- SIEBE 50816/66
РНР		_									
PHP PHP is a gener which case PH					especial	y suited t	to serv	ver-s	side web	develop	ment, in
NA	18/07	7/2016	5.1	PHP throw attempt to section 4.1 conflicts a protect ap presence of data in the environme might allor redirect an outbound arbitrary p crafted Pro- HTTP requ by (1) an a makes a ge call or (2) PHP, aka a	address 1.18 nam nd there plication of untrus e HTTP_P ent varia w remote n applica proxy ser oxy head uest, as d application etenv('H' a CGI com in "httpo	RFC 387 espace fore does s from the ted client ROXY ole, which e attacken tion's offic to an ver via a er in an emonstra on that TTP_PRO figuratic ky" issue.	5 not ne t h rs to n ated XY') on of	ed	tps://bu hat.com/ ug.cgi?id 4	'show	A-PHP- PHP 50816/67
Denial of Service; Overflow	25/07	7/2016	6.8	Integer ov php_stream function in in PHP bef before 5.6 7.0.9 allow	rerflow in m_zip_op n ext/zip, fore 5.5.3 .24, and 2	the ener /zip_strea 8, 5.6.x 7.x before	am.c		tps://bu 1et/7252		A-PHP- PHP 50816/68
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10

			cause a denial of service (stack- based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL. Reference: CVE-2016-6297		
Denial of Service; Overflow	25/07/2016	7.5	Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap- based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function. Reference: CVE-2016-6296	https://bugs.ph p.net/72606	A-PHP- PHP 50816/69
Denial of Service	25/07/2016	7.5	ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use- after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773. Reference: CVE-2016-6295	https://bugs.ph p.net/72479	A-PHP- PHP 50816/70
Denial of Service	25/07/2016	7.5	The locale_accept_from_http function in ext/intl/locale/locale_methods. c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTT P function, which allows remote	https://bugs.ph p.net/72533	A-PHP- PHP 50816/71

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

			attackers t service (or possibly h impact via argument. Reference	ut-of-bou ave unsp a call wi	nds read ecified ot th a long) or ther				
Denial of Service	25/07/2016	4.3	The exif_p function in PHP befor 5.6.24, and allows rem cause a de pointer de applicatio JPEG imag Reference	n ext/exif e 5.5.38, d 7.x befonote attae nial of se referenc n crash) e.	Vexif.c in 5.6.x before re 7.0.9 ckers to rvice (NU e and via a craft	ore JLL ted		tps://bu 1et/7261		A-PHP- PHP 50816/72
Denial of Service; Overflow Memory Corruption; Gain Information	25/07/2016	7.5	The exif_proce TE functio PHP befor 5.6.24, and allows ren cause a de of-bounds memory c sensitive i process m have unsp via a crafte Reference	n in ext/ e 5.5.38, l 7.x befo note attac nial of se array ac orruption nformati emory, o ecified of ed JPEG i	exif/exif. 5.6.x before re 7.0.9 ckers to rvice (ou cess and n), obtain on from r possibly cher impa- mage.	c in ore t- y act		tps://bu iet/7260		A-PHP- PHP 50816/73
Denial of Service	25/07/2016	7.5	ext/sessio before 5.5 5.6.24, and not proper hash data allows ren cause a de after-free) unspecifie vectors re deserializa Reference	.38, 5.6.x d 7.x befor rly maint structure note attac nial of se or possi d other i lated to s ation.	before re 7.0.9 c ain a cert e, which ckers to rvice (us bly have mpact via ession	loes cain e-		tps://bu៛ 1et/7256		A-PHP- PHP 50816/74
Denial of	25/07/2016	6.8	Integer ov			U	htt	tps://bu	gs.ph	A-PHP-
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10

Siemens Simatic Batch;	Simatic Ope	enpcs 7;		tic Winco		10 1022					
Siemens						10 1022					
Execute Code; SQL Injection	27/07/20		be in lo ea ob un Ra SC Fa be at SC ve	actoryTall efore 2.20 validate o gout action sier for r otain accent attended eference QL injection ockwell A actoryTall efore 2.20 tackers to QL comma ectors. eference	0.00 does credentia on, which emote at ss by lev worksta CVE-20 on vulner utomatic k Energy 0.00 allow execute ands via t	not ls upon a makes it tackers to eraging a tion. 16-4531 rability in m Metrix as remote arbitrary	t o in i v e y ed	cer es/ 03 htt cer ies	rt.us- rt.gov/ac /ICSA-16	lvisori -173- - lvisor	FACTO 50816/77 A-ROC- FACTO 50816/78
Factorytalk En FactoryTalk En energy informa NA	ergrymetri ergyMetrix is	s a web-e tually ar	ny loca		-		ickage		nt gives y		<i>ss to critical</i> A-ROC-
Denial of Service; Overflow Rockwellauto	25/07/20	16 7.5	F T in b a s p in s	Reference The php_u n ext/stan before 5.5 ttackers t ervice (br oossibly h mpact via mart_str Reference	e: CVE-20 rl_parse_ ndard/ur .38 allow to cause a uffer ove ave unsp vectors data type	16-628 ex functi l.c in PHI s remote denial o c-read) o ecified ot nvolving	on of r ther g the		p://php ngeLog-		A-PHP- PHP 50816/76
			T P 5 a c b p p ii	SRM/tsr PHP befor 6.6.24, and llows ren ause a de based buff bossibly h mpact via operation	e 5.5.38, l 7.x befo note attac nial of se er overfl ave unsp a crafteo	_cwd.c ir 5.6.x before 7.0.9 ckers to rvice (statow) or ecified of l extract	ore ack-	p.n	iet/7251	3	PHP 50816/75

The SIMATIC BATCH software can be used to implement even the most complex batch processes effectively and at a reasonable cost; OpenPCS V.7 is the version of our IEC 61131-3-compliant programming environment for the development of control applications which has proven its worth on the market; SIMATIC WinCC is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) system from Siemens.

system from S	iemens.										
Exec Code	22/07	/2016	7 U b d t 0 a: t 0 a: 8 R 8 R S a c	iemens SI .3 Update pdate 1, S efore 8.1 S istributed nrough 8.1 penPCS 7 s distribut nrough 8.1 penPCS 7 s distribut .2, and SIN .untime Pr P1 Update ttackers to ode via cra	10 and 7 IMATIC I SP1 Upda in SIMA SP1, SIM before 8 ced in SIM before 8 ced in SIM MATIC W rofession 9 allow o execute afted pac	.4 before BATCH te 9 as FIC PCS 7 IATIC 1 Update IATIC PC IATIC 2 Update IATIC PC inCC al before remote arbitrary kets.	e 3 S 7 e 1 S 7 13 y	me po ns so	tp://ww ens.com/ ol/cert/s _security ry_ssa- 8531.pd	'cert/ sieme r_advi	A-SIE- SIMAT 50816/79
Simatic Net I The SIMATIC			lør Editio	n 2008 is 1	oloasod f	or uso in	SIMO	TIO	Nannlica	tions	
Denial of		, 		iemens SI			SINO	1	tp://ww	1	A-SIE-
Service	22707	/2010	S re d o	oftware b emote atta enial of se utage) via	efore 13 ackers to rvice (OI crafted 7	SP2 allov cause a PC UA ser FCP pack	vice ets.	me po ns so	ens.com/ ol/cert/s _security ry_ssa- 3276.pd	'cert/ sieme r_advi	SIMAT 50816/80
Simatic Wind SIMATIC Wind system from S	CC is a sup	ervisory	control a	nd data a	cquisitior	(SCADA)) and		-		erface (HMI)
		/2016	th re a c	iemens SI nrough SP emote atta rbitrary W rafted pac A eference	3 and 7.2 ackers to /inCC sta kets.	allows read tion files	via	mo po ns or	tp://ww ens.com/ ol/cert/s _security y_ssa- 8531.pd	′cert/ sieme r_advis	A-SIE- SIMAT 50816/81
Sinema Rem The new man SINEMA Remo maintenance.	agement p	latform	<mark>er</mark> for remot	te network	s, SINEM	A Remote	e Conr	nect	, is a serv	er appli	
CV Scoring	0-1	1-2	2-3	3-4	4-5	<mark>5-6</mark>	6-2	7	7-8	8-9	9-10

Scale

XSS	22/07/2016	4.3	Cross-site s vulnerabili web server Remote Co 1.2 allows r inject arbit HTML via a Reference	ty in the in Sieme nnect Ser remote at rary web crafted l	integrate ens SINEN ever befor tackers t script or JRL.	MA re co	me /p me ad	p://www ens.com/ ool/cert/ ens_secur visory_ss 9132.pdf	cert /sie rity_ a-	A-SIE- SINEM 50816/82
Vtiger										
CRM										
Vtiger CRM is a p					· · · · · · · · · · · · · · · · · · ·		·			Γ
NA	31/07/2016	5.5	modules/U p in Vtiger does not pr save action remote aut create or m via unspeci Reference	CRM 6.4. operly re s, which henticate odify use fied vect	0 and ear estrict use allows ed users t er account ors.	rlier er- to its	er. tig it/ b4	p://code com/vtig ercrm/co 7cdf9942 aa58114 ce88fb41 c	ger/v omm 1197 eafc	A-VTI-CRM- -50816/83
Xmlsoft										
Libxml2										
libxml2 is a softv	ware library for	parsing	g XML docun	nents.						
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in A 9.3.3, OS X iTunes befor Windows, i Windows, i watchOS be remote atta denial of se corruption unspecified unknown v vulnerabili 4614, CVE- 2016-4616 Reference	before 10 ore 12.4.2 Cloud be vOS befo efore 2.2. ackers to rvice (ma) or possi l other in rectors, a ty than C 2016-46 CVE-20).11.6, 2 on fore 5.2.1 re 9.2.2, 3 2 allows cause a emory bly have pact via different VE-2016 15, and C 16-4619	and - VE-	.ap 06	ps://sup ple.com/ 905	/HT2	A-XML- LIBXM 50816/84
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in A 9.3.3, OS X iTunes befo Windows, i on Window and watch(before 1(ore 12.4.2 Cloud be vs, tvOS b).11.6, 2 on fore 5.2.1 efore 9.2		-	os://sup le.com/I)5	-	A-XML- LIBXM 50816/85
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

			allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016- 4615, and CVE-2016-4619. Reference: CVE-2016-4616		
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016- 4616, and CVE-2016-4619. Reference: CVE-2016-4615	https://support. apple.com/HT20 6905	A-XML- LIBXM 50816/86
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4615, CVE-2016- 4616, and CVE-2016-4619. Reference: CVE-2016-4614	https://support. apple.com/HT20 6905	A-XML- LIBXM 50816/87

Libxslt is the XSLT C library developed for the GNOME project. XSLT itself is a an XML language to define
transformation for XML.Denial of21/07/20167.5libxslt in Apple iOS before 9.3.3.https://support.A-XML-

Denial of	21/0/	/2016	/.5 III	oxsit in Aj	pple iUS i	before 9.	3.3, ntt	ps://sup	port. A	-XML-
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Service; Overflow Memory Corruption			OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows	apple.com/HT20 6905	LIBXS 50816/88
			remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016- 4607, CVE-2016-4608, CVE- 2016-4609, and CVE-2016- 4610.		
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	Reference: CVE-2016-4612 libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016- 4607, CVE-2016-4608, CVE- 2016-4609, and CVE-2016- 4612. Reference: CVE-2016-4610	https://support. apple.com/HT20 6905	A-XML- LIBXS 50816/89
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-	https://support. apple.com/HT20 6905	A-XML- LIBXS 50816/90

CV Scoring 0-1 Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
-------------------------	-------	-----	-----	-----	-----	-----	-----	-----	------

			2 4	607, CVE- 016-4610 612. eference	, and CVE	2-2016-				
Denial of Service; Overflow Memory Corruption	21/07/2	2016	0 bu iC W w re du co u u u u v v 4 4 2 4	bxslt in Aj S X before efore 12.4 Cloud befo Vindows, t vatchOS be emote atta enial of se orruption nspecified nknown v ulnerabili 607, CVE- 016-4610 612. eference	2 10.11.6, .2 on Win re 5.2.1 o vOS befo efore 2.2. ockers to rvice (me) or possi l other im ectors, a ty than C 2016-460 , and CVE	iTunes ndows, on 2 allows cause a emory bly have pact via different VE-2016- 09, CVE- 5-2016-	and -	tps://supj pple.com/I 904	HT20	A-XML- LIBXS 50816/91
Denial of Service; Overflow Memory Corruption	21/07/2	2016	0 bu iC W w re du co u u u u v v 4 4 2 4	bxslt in Aj S X before efore 12.4 Cloud befo Vindows, t vatchOS be emote atta enial of se orruption nspecified nknown v ulnerabili 608, CVE- 016-4610 612. eference	2 10.11.6, .2 on Win re 5.2.1 o vOS befo efore 2.2. ockers to rvice (mo) or possi l other im ectors, a ty than C 2016-460 , and CVE	iTunes ndows, on re 9.2.2, a 2 allows cause a emory bly have npact via different VE-2016- 09, CVE- 2-2016-	and -	tps://supj pple.com/H 905	HT20	A-XML- LIBXS 50816/92
		A	pplicat	ion;Ope	rating S	System	(A/OS))		
Apple/AppleApple Tv;Iphone Os/SafariApple TV is a digital media player and a microconsole developed and sold by Apple Inc; iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware/ Safari is a web browser developed by Apple based on the WebKit engine.										
Denial of	21/07/2	2016	6.8 W	/ebKit in / 3-4	apple iOS	petore 9	.3.3, h	ttps://sup	port	A-OS-APP-

Service; Execute Code; Overflow; Memory Corruption			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-2016-4622, and CVE- 2016-4623. Reference: CVE-2016-4624	.apple.com/HT2 06905	APPLE 50816/93
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	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-2016-4622, and CVE- 2016-4624. Reference: CVE-2016-4623	https://support .apple.com/HT2 06905	A-OS-APP- APPLE 50816/94
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	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. Reference: CVE-2016-4622	https://support .apple.com/HT2 06905	A-OS-APP- APPLE 50816/95
Cross Site Scripting	21/07/2016	4.3	Cross-site scripting (XSS) vulnerability in the WebKit JavaScript bindings in Apple iOS before 9.3.3 and Safari before 9.1.2 allows remote attackers to inject arbitrary web script or HTML via a crafted HTTP/0.9 response, related to a "cross- protocol cross-site scripting (XPXSS)" vulnerability. Reference: CVE-2016-4651	https://support .apple.com/HT2 06902	A-OS-APP- IPHON 50816/96

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

Canonical/Ecryptfs

Ubuntu Linux/Ecryptfs-utils

Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers/ The ecryptfs-utils package provides several different ways of setting up eCryptfs.

NA	22/07/2016	2.1	ecryptfs-setup-swap in eCryptfs does not prevent the unencrypted swap partition from activating during boot when using GPT partitioning on a (1) NVMe or (2) MMC drive, which allows local users to obtain sensitive information via unspecified vectors. NOTE: this vulnerability exists because of on incomplete fur for CVE 2015	https://bazaar.la unchpad.net/~ec ryptfs/ecryptfs/t runk/revision/8 82	A-OS-CAN- UBUNT 50816/97				
			an incomplete fix for CVE-2015- 8946. Reference: CVE-2016-6224						
Annlo			Operating System(OS)						
Apple Apple Ty:Ipho	one Os;Mac Os X	(Watc	hos						
Apple TV is a di	igital media play	er and	a microconsole developed and sold b						
<i>iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware; OS X (originally Mac OS X) is a series of Unix-based graphical interface operating systems</i>									
(OS) developed	(OS) developed and marketed by Apple Inc; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.								

developed by A	<i>ipple inc.</i>											
Denial of	21/07	/2016	7.2	The kernel	in Apple	iOS befor	re	htt	ps://sup	port	0-	APP-
Service;				9.3.3, OS X	before 10	OS	.apple.com/HT2			AI	PPLE	
Overflow;				before 9.2.2	2, and wa	tchOS be	fore	06905			50)816/98
Gain				2.2.2 allows	s local us	ers to gai	in					
Privileges;				privileges o	or cause a	denial o	f					
Memory				service (me	emory co	rruption) via					
Corruption				unspecified	l vectors,	a differe	nt					
				vulnerabili	ty than C	VE-2016	-					
				1863 and C	VE-2016	-4582.						
				Reference	: CVE-20							
Denial of	21/07	/2016	6.8	CoreGraph	ics in App	ole iOS		htt	ps://sup	port	0-	APP-
Service;				before 9.3.3	3, OS X be	fore 10.1	1.6,	.apple.com/HT2			AI	PPLE
Execute Code;				tvOS before	e 9.2.2, ar	nd watch	OS	06	905		50)816/99
Overflow;				before 2.2.2	2 allows i	emote						
Memory				attackers to	o execute	arbitrar	y					
Corruption				code or cau	ise a deni	al of serv	vice					
				(memory c	orruption							
				crafted BM	P image.							
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	,	7-8	8-9		9-1 0
L												

			Reference	: CVE-20	16-4637	7					
Denial of Service; Overflow	21/07/2016		ImageIO in 9.3.3, OS X before 9.2.2 2.2.2 allow cause a der (memory c unspecified Reference	before 10 2, and wa s remote nial of ser onsumpt l vectors.	OS efore s to	.ap	tps://sup ople.com/ 905			PP- 'LE 16/100	
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	5 6.8	ImageIO in 9.3.3, OS X before 9.2.2 2.2.2 allow execute art denial of se corruption file. Reference	before 10 2, and wa s remote bitrary co ervice (m) via a cra).11.6, tv tchOS be attackers de or cau emory afted TIF	OS efore s to use a F	.ap	tps://sup pple.com/ 905	-		PP- 'LE 16/101
Denial of Service; Gain Privileges	21/07/2016	5 7.2	IOHIDFamily in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors.					https://support .apple.com/HT2 06905			PP- 'LE 16/102
NA	21/07/2016	6 4.6	Reference: CVE-2016-4626 The Sandbox Profiles component in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows attackers to access the process list via a crafted app that makes an API call. Reference: CVE-2016-4594					https://support .apple.com/HT2 06905			PP- PLE 16/103
Denial of Service; Overflow Gain Privileges; Memory Corruption	21/07/2016	5 7.2	The kernel 9.3.3, OS X before 9.2.2 2.2.2 allow privileges of service (me unspecified vulnerabili	before 10 2, and wa s local us or cause a emory co l vectors,	OS efore in of) via ent	https://support .apple.com/HT2 06904				PP- PLE 16/104	
CV Scoring Scale	0-1 1-2	2-3	3 3-4	4-5	5-6	6-7	7	7-8	8-9		9-1 0

Aallows local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors. Reference: CVE-2016-4627IIphone Os iOS (originally iPhone OS) is a mobile pertating system created and developed by Apple Inc. and distribut exclusively for Apple hardware: 21/07/20167.1Calendar in Apple iOS before 9.3.3 allows remote attackers to cause a denial of service (NULL pointer dereference and developed restartly via a crafted invitation. Reference: CVE-2016-4605https://support apple.com/HT2 069020-APP- 1PHON 50816/1Bypass; Gain Information21/07/20164.3Web Media in Apple iOS before restartly via a crafted invitation. Reference: CVE-2016-4605https://support apple.com/HT2 069020-APP- 1PHON 50816/1Bypass; Gain Information21/07/20164.3Web Media in Apple iOS before omechanism and obtain sensitive video URL information by leveraging Safari View Controller misbehavior. Reference: CVE-2016-4603https://support apple.com/HT2 069020-APP- 1PHON 50816/121/07/20162.1The Siri Contacts component in information via unspecified vectors. Reference: CVE-2016-4503https://support apple.com/HT2 069020-APP- 1PHON 50816/11050riginally iPhone 0S) is a mobile pertating system created and developed by Apple Inc. and distribut exclusively for Apple hardware; US (originally iPhone 0S) is a mobile pertating system created and developed by Apple Inc. and distribut exclusively for Apple hardware; US (originally iPhone 0S) is a mobile pertating system created and developed by Apple Inc. and distribut exclusively for Apple hardware; US					1863 and 0 Reference						
Denial of Service21/07/20167.1Calendar in Apple iOS before 9.3.3 allows remote attackers to cause a denial of service (NULL 	Service; Gain Privileges Iphone Os <i>iOS (originally</i>	iPhone OS	5) is a m		iOS before 9.2.2, and v allows loca privileges of service (NU dereferenc vectors. Reference	9.3.3, tvC vatchOS l users to or cause a JLL point e) via uns : CVE-20	S before before 2.2 gain denial o er specified 16-4627	.apple.con 06905	n/HT2	APPLE 50816/105	
Service9.3.3 allows remote attackers to cause a denial of service (NULL pointer dereference and device restart) via a crafted invitation. Reference: CVE-2016-4605.apple.com/HT2 06902IPHON 50816/1Bypass; Gain Information21/07/20164.3Web Media in Apple iOS before 9.3.3 allows attackers to bypass the Private Browsing protection mechanism and obtain sensitive video URL information by leveraging Safari View Controller misbehavior. Reference: CVE-2016-4603https://support 069020-APP- 1PHON 50816/121/07/20162.1The Siri Contacts component in Apple iOS before 9.3.3 allows physically proximate attackers to read arbitrary Contact card information via unspecified vectors. Reference: CVE-2016-4593https://support .apple.com/HT20-APP- .Iphone Os;Mac Os X i0S (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distribute exclusively for Apple hardware; OS X (originally Mac OS X) is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. allows man-in-the-middlehttps://support .apple.com/HT20-APP- .apple.com/HT2NA21/07/20163.5 FaceTime in Apple iOS before 9.3.3 and OS X before 10.11.6 allows man-in-the-middlehttps://support .apple.com/HT20-APP- .apple.com/HT2				7.1	Calendar i	n Apple i)S before	9	https://su	ipport	O-APP-
InformationInformati	Service				9.3.3 allow cause a der pointer de restart) via Reference	vs remote nial of se reference a a crafte e: CVE-20	attacker vice (NU and dev l invitati 16-460	rs to JLL ice on. 5	apple.con 06902	n/HT2	IPHON 50816/106
Apple iOS before 9.3.3 allows physically proximate attackers to read arbitrary Contact card information via unspecified vectors. Reference: CVE-2016-4593.apple.com/HT2 06902IPHON 50816/1Iphone Os;Mac Os X iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distribut exclusively for Apple hardware; OS X (originally Mac OS X) is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inchttps://support .apple.com/HT2O-APP- .apple.com/HT2NA21/07/20163.5FaceTime in Apple iOS before 9.3.3 and OS X before 10.11.6 allows man-in-the-middlehttps://support .ope03O-APP- .39816/1		21/07,	/2016	4.3	9.3.3 allow the Private mechanism video URL leveraging Controller	e Browsin and obt informat Safari Vi misbeha	rs to byp g protec ain sensi ion by ew vior.	ass tion tive	.apple.con		
iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distribut exclusively for Apple hardware; OS X (originally Mac OS X) is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc NA 21/07/2016 3.5 FaceTime in Apple iOS before 9.3.3 and OS X before 10.11.6 allows man-in-the-middle 06903 0-APP- 1PHON 50816/1		21/07,	/2016	2.1	The Siri Contacts component in Apple iOS before 9.3.3 allows physically proximate attackers to read arbitrary Contact card information via unspecified vectors.				.apple.con		
NA21/07/20163.5FaceTime in Apple iOS before 9.3.3 and OS X before 10.11.6 allows man-in-the-middlehttps://support .apple.com/HT20-APP- IPHON 50816/1	iOS (originally exclusively for	iPhone OS Apple hard	dware; (OS X (oi	perating sys riginally Ma	tem creat c OS X) is	ed and de a series o	evelop			
			_		FaceTime 9.3.3 and C allows man	in Apple)S X befo n-in-the-	OS befor e 10.11. niddle	6	.apple.con	-	

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1 0
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	--------------

	termination, and obtain	
	· ·	
	sensitive audio information in	
	opportunistic circumstances, via	
	unspecified vectors.	
	Reference: CVE-2016-4635	

Iphone Os;Watchos

iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.

inppic me.					
Denial of	21/07/2016	4.9	IOAcceleratorFamily in Apple	https://suppor	O-APP-
service; Gain			iOS before 9.3.3 and watchOS	t.apple.com/HT	IPHON
Information			before 2.2.2 allows local users to	206904	50816/110
			obtain sensitive information		
			from kernel memory or cause a		
			denial of service (out-of-bounds		
			read) via unspecified vectors.		
			Reference: CVE-2016-4628		

Mac Os X

OS X (originally Mac OS X) is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc.

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9		9-10
Denial of	21/07	7/2016	7.2	Audio in A	pple OS X	before		ht	tps://suj	ppor	0-	APP-MAC
Denial of service; Gain Information	21/07	7/2016	4.9	Audio in A 10.11.6 allo obtain sense layout info denial of se read) via u Reference	pple OS X ows local sitive ker rmation ervice (ou nspecifie	before users to nel mem or cause ut-of-bou	ory- a nds s.	t.a	tps://suj pple.com 6903		0	APP-MAC - 816/113
Denial of Service	21/07	7/2016	2.1	Audio in A 10.11.6 all cause a der pointer der unspecifier Reference	ows local nial of ser reference d vectors	users to rvice (NU e) via	LL	t.a	tps://suj pple.com 06903		0	APP-MAC - 816/112
Denial of Service; Gain Privileges; Gain Information	21/07	7/2016	3.3	CoreGraph before 10.2 to obtain s from kerne consequen cause a den bounds rea vectors. Reference	l 1.6 allow ensitive i el memor tly gain p nial of sen ad), via un	vs local u nformati y and privileges rvice (ou nspecifie	on , or t-of- d	t.a	tps://suj pple.com 6903		0	APP-MAC - 816/111

Service;			10.11.6 allows local users to	t.apple.com/HT	0
Overflow; Gain			gain privileges or cause a denial	206903	50816/114
Privileges;			of service (memory corruption)		
Memory			via a crafted file.		
Corruption			Reference: CVE-2016-4647		
Denial of	21/07/2016	4.3	Audio in Apple OS X before	https://suppor	O-APP-MAC
service; Gain			10.11.6 mishandles a size value,	t.apple.com/HT	0
Information			which allows remote attackers	206903	50816/115
			to obtain sensitive information		
			or cause a denial of service (out-		
			of-bounds read) via a crafted		
			audio file.		
NT A	21/07/2016	2.1	Reference: CVE-2016-4646		
NA	21/07/2016	2.1	CFNetwork in Apple OS X before	https://suppor	O-APP-MAC
			10.11.6 uses weak permissions	t.apple.com/HT	0
			for web-browser cookies, which allows local users to obtain	206903	50816/116
			sensitive information via		
			unspecified vectors.		
			Reference: CVE-2016-4645		
Execute Code;	21/07/2016	9.3	Login Window in Apple OS X	https://suppor	O-APP-MAC
Gain	21/0//2010	2.5	before 10.11.6 allows attackers	t.apple.com/HT	0
Information			to execute arbitrary code in a	206903	50816/117
			privileged context or obtain	200900	00010/11/
			sensitive user information via a		
			crafted app that leverages a		
			"type confusion."		
			Reference: CVE-2016-4641		
Dejnial of	21/07/2016	9.3	Login Window in Apple OS X	https://suppor	O-APP-MAC
Service;			before 10.11.6 allows attackers	t.apple.com/HT	0
Execute Code;			to execute arbitrary code in a	206903	50816/118
Overflow;			privileged context, obtain		
Memory			sensitive user information, or		
Corruption;			cause a denial of service		
Gain			(memory corruption) via a		
Information			crafted app.		
			Reference: CVE-2016-4640		
Denial of	21/07/2016	4.4	Login Window in Apple OS X	https://suppor	O-APP-MAC
Service			before 10.11.6 does not properly	t.apple.com/HT	0
			initialize memory, which allows	206903	50816/119
			local users to cause a denial of		
			service via unspecified vectors.		
			Reference: CVE-2016-4639		

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

NA	21/07/2016	9.3	Login Window in Apple OS X before 10.11.6 allows attackers to gain privileges via a crafted app that leverages a "type confusion." Reference: CVE-2016-4638	https://suppor t.apple.com/HT 206903	O-APP-MAC O 50816/120
Denial of Service; Overflow; Gain Privileges; Memory Corruption	21/07/2016	7.2	The Graphics Drivers subsystem in Apple OS X before 10.11.6 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors. Reference: CVE-2016-4634	https://suppor t.apple.com/H T206903	O-APP-MAC O 50816/121
Denial of Service; Execute Code; Memory Corruption	21/07/2016	6.9	Intel Graphics Driver in Apple OS X before 10.11.6 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. Reference: CVE-2016-4633	https://suppor t.apple.com/H T206903	O-APP-MAC O 50816/122
DoS Exec Code Overflow Mem. Corr.	21/07/2016	6.8	ImageIO in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted EXR image with B44 compression. Reference: CVE-2016-4630	https://suppor t.apple.com/H T206903	O-APP-MAC O 50816/123
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	10	ImageIO in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted xStride and yStride values in an EXR image. Reference: CVE-2016-4629	https://suppor t.apple.com/H T206903	O-APP-MAC O 50816/124
NA	21/07/2016	7.2	Use-after-free vulnerability in IOSurface in Apple OS X before 10.11.6 allows local users to gain privileges via unspecified vectors. Reference: CVE-2016-4625	https://suppor t.apple.com/H T206903	O-APP-MAC O 50816/125

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

Service;			10.11.6 allows remote attackers	t.apple.com/H	0
Memory Corruption Denial of	21/07/2016	6.8	(memory corruption) via a crafted Photoshop document. Reference: CVE-2016-4599 QuickTime in Apple OS X before	https://suppor	0-APP-MA
Overflow;			cause a denial of service	1200703	
Execute Code;			to execute arbitrary code or	T206903	50816/130
Service;		0.0	10.11.6 allows remote attackers	t.apple.com/H	0
Denial of	21/07/2016	6.8	Reference: CVE-2016-4600 QuickTime in Apple OS X before	https://suppor	O-APP-MA
			CVE-2016-4602.		
			2016-4596, CVE-2016-4597, and		
Corruption			crafted FlashPix bitmap image, a different vulnerability than CVE-		
Memory			(memory corruption) via a		
Overflow;			cause a denial of service		
Execute Code;			to execute arbitrary code or	T206903	50816/129
Service;			10.11.6 allows remote attackers	t.apple.com/H	0
Denial of	21/07/2016	6.8	QuickTime in Apple OS X before	https://suppor	O-APP-MA
			Reference: CVE-2016-4601		
Corruption			crafted SGI image.		
Memory			(memory corruption) via a		
Execute Code; Overflow;			to execute arbitrary code or cause a denial of service	1200903	50816/128
Service;			10.11.6 allows remote attackers	t.apple.com/H T206903	0
Denial of	21/07/2016	6.8	QuickTime in Apple OS X before	https://suppor	O-APP-MA
	04/07/2011		Reference: CVE-2016-4602		
			CVE-2016-4600.		
			2016-4596, CVE-2016-4597, and		
1 -			different vulnerability than CVE-		
Corruption			crafted FlashPix bitmap image, a		
Memory			(memory corruption) via a		
Execute Code; Overflow;			to execute arbitrary code or cause a denial of service	1200903	50816/127
Service;			10.11.6 allows remote attackers	t.apple.com/H T206903	0
Denial of	21/07/2016	6.8	QuickTime in Apple OS X before	https://suppor	O-APP-MA
			Reference: CVE-2016-4621		
Corruption			corruption) via a crafted app.		
Memory			denial of service (memory		
Overflow;			privileged context or cause a		
Execute Code;			execute arbitrary code in a	t.apple.com/H T206903	50816/12
Service;			10.11.6 allows attackers to	Labole.com/ 🗖	0

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

Execute Code;			to execute				T20	6903		50	816/131
Overflow;			cause a de								
Memory Corruption			(memory o crafted im	-	nj vla a						
Corruption			Reference	0	16.459	8					
Denial of	21/07/201		QuickTime				httn	s://su	nnor	0-/	APP-MAC
Service;	21/0//201	0.0	10.11.6 all				-	ole.cor		0	_
Execute Code;			to execute					6903	,	-	816/132
Overflow;			cause a de								,
Memory			(memory o	corruptio	n) via a						
Corruption			crafted Fla	shPix bit	map ima	ge, a					
-			different v	ulnerabil	ity than	CVE-					
			2016-4596	6, CVE-20	16-4600	, and					
			CVE-2016								
			Reference	e: CVE-20	016-459	7					
Denial of	21/07/201		QuickTime				_	s://su		-	APP-MAC
Service;			10.11.6 all					ole.cor	n/H	0	
Execute Code;			to execute				T20	6903		50	816/133
Overflow;			cause a de								
Memory			(memory of	-	-						
Corruption			crafted Fla		-	0					
			different v								
			2016-4592 CVE-2016		10-4000	, and					
			Reference		016-459	6					
NA	21/07/201		Safari Logi				http	s://su	ppor	0-4	APP-MAC
			X before 1				_	ole.cor		0	
			physically	proxima	te attacke	ers	T20	6903		50	816/134
			to discove	r passwo	rds by						
			reading th		during th	ie					
			login proc								
			Reference	e: CVE-20	016-459	5					
Oracle											
Integrated Ligh		U				, .	, , ,				4.0.0
Oracle Integrated	0	0 (-						Jracle	s SP.	ARL
Enterprise T-seri NA	<u>es and Sun Fl</u> 21/07/201			fied vulne				: ://ww	MALOY	0.0	DRA-
11/1	21/0//201	0 9	-	lea vuine I compor			-	://ww com/t			JRA- TEG
				ems Proc				ork/se			816/135
			-	and 3.2 a			y-	, i ky se	curit	500	510/155
				cated use				sory/o	couiu		
	1			tiality, in			1201		puju		
								-		1	
					ctors rela	ated	288	1720.ł	ntml		
CV Scoring	0-1 1-2	2 2-3		ity via ve	ctors rela	ated 6-7	288	1720.ł 7-8	ntml 8-9		9-10

			to LUMAIN. Reference: CVE-2016-5457		
NA	21/07/2016	7.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to IPMI. Reference: CVE-2016-5453	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-ORA- INTEG 50816/136
NA	21/07/2016	5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect availability via vectors related to Console Redirection. Reference: CVE-2016-5449	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-ORA- INTEG 50816/137
NA	21/07/2016	6.4	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect integrity and availability via vectors related to SNMP. Reference: CVE-2016-5448	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-ORA- INTEG 50816/138
NA	21/07/2016	6.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors. Reference: CVE-2016-5447	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-ORA- INTEG 50816/139
NA	21/07/2016	7.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	O-ORA- INTEG 50816/140

CV Scoring 0-1 1-2 Scale	2-3 3-4	4-5 5-6	6-7 7-8	8-9	9-10
-----------------------------	---------	---------	---------	-----	------

			to Infrastructure. Reference: CVE-2016-5446		
NA	21/07/2016	7.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. Reference: CVE-2016-5445	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-0RA- INTEG 50816/14
Solaris Oracle Sola Solaris OS.	ris Cluster provides hi	gh availd	ability for enterprise applications a	nd databases on t	heOracle
NA	21/07/2016	2.1	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect availability via vectors related to Kernel, a different vulnerability than CVE-2016-3497 and CVE- 2016-5469. Reference: CVE-2016-5471	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-0RA- SOLAR 50816/14
NA	21/07/2016	2.1	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect availability via vectors related to Kernel, a different vulnerability than CVE-2016-3497 and CVE- 2016-5471. Reference: CVE-2016-5469	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-0RA- SOLAR 50816/14
NA	21/07/2016	5.4	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect integrity and availability via vectors related to Verified Boot. Reference: CVE-2016-5454	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016- 2881720.html	0-0RA- SOLAR 50816/14
NA	21/07/2016	2.1	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect confidentiality via vectors related to Verified Boot. Reference: CVE-2016-5452	http://www.o racle.com/tech network/secur ity- advisory/cpuj ul2016-	0-0RA- SOLAR 50816/14

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

2881720.html

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
---------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------