

			Reader DC Continuous be 15.020.20039 Windows and allow attacker execute arbitra code or cause a denial of servic (memory corruption) via unspecified ve Reference: CV 2016-4095	on OS X s to ary a ce actors.				
Connect			2010 1075					
Adobe Connect w					ve online	e meeting o	experie	nces for
collaboration, virt	08/11/2016	4.3	Adobe Connect version 9.5.6 at earlier does not adequately valuately input in the expressivation must be a could be explosin cross-site scripting attact Reference: CV 2016-7851	t ind ot idate ents odule. lity ited	obe.com		A-AD CONN 1811	
Flash Player								
Adobe Flash Play								
including viewing Execute Code	01/11/2016	10	Use-after-free vulnerability in Adobe Flash Plash Plas	n layer 205 on OS X on emote eccute via ctors, the	https:// obe.com y/produ	helpx.ad securit acts/flash apsb16-	A-AD FLAS	0-
CV Scoring O-Scale	-1 1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

				erence: (.6-7855	CVE-				
Flash Player; Fla									
Adobe Flash Play									
including viewing					plication	is, and sti	reaming v	ideo an	d audio;
Flash Player is als Execute Code	08/11/2016	10	_	be Flash	Plaver	https://	helpx.ad	A-AD	O-
Execute Gode	00/11/2010			sions 23.0	-		1/securit	FLAS	
				earlier,			icts/flash		16/05
			11.2	2.202.643	and	-player,	/apsb16-		-
				ier have a		37.html			
			_	loitable ty	/pe				
				fusion ierability.					
				cessful	•				
				loitation (could				
			_	l to arbitr					
				e executio					
				erence: (CVE-				
Execute Code	00/11/2016	10		6-7865	Dlavon	https://	/holov od	A-AD	0
Execute Code	08/11/2016	10		be Flash i sions 23.0	•		helpx.ad securit	FLAS	
				earlier,	7.0.203		i/seedi ie icts/flash		16/06
				2.202.643	and	· · ·	/apsb16-		,
			earl	ier have a	an	37.html			
			_	loitable u	se-				
				r-free					
				nerability cessful					
				loitation (could				
			_	l to arbitr					
				e executio					
				erence: (CVE-				
	00/11/2001	4.0		6-7864	D.		<i>(</i>) 1 -		
Execute Code	08/11/2016	10		be Flash is sions 23.0		. , ,	helpx.ad securit	A-AD FLAS	
				earlier,	1.0.205		i/securit icts/flash	_	п 16/07
				2.202.643	and		/apsb16-	1011	10/07
				ier have a		37.html			
				loitable u					
				r-free					
				nerability.					
				cessful Loitation	could				
			_	loitation o l to arbitr					
						· 			
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			code execution. Reference: CVE- 2016-7863		
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable useafter-free vulnerability. Successful exploitation could lead to arbitrary code execution. Reference: CVE-2016-7862	https://helpx.ad obe.com/securit y/products/flash -player/apsb16- 37.html	A-ADO- FLASH 181116/08
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. Reference: CVE-2016-7861	https://helpx.ad obe.com/securit y/products/flash -player/apsb16- 37.html	A-ADO- FLASH 181116/09
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. Reference: CVE-2016-7860	https://helpx.ad obe.com/securit y/products/flash -player/apsb16- 37.html	A-ADO- FLASH 181116/10

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

Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable useafter-free vulnerability. Successful exploitation could lead to arbitrary code execution. Reference: CVE-2016-7859	https://helpx.ad obe.com/securit y/products/flash -player/apsb16- 37.html	A-ADO- FLASH 181116/11
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable useafter-free vulnerability. Successful exploitation could lead to arbitrary code execution. Reference: CVE-2016-7858	https://helpx.ad obe.com/securit y/products/flash -player/apsb16- 37.html	A-ADO- FLASH 181116/12
Execute Code Artifex	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable useafter-free vulnerability. Successful exploitation could lead to arbitrary code execution. Reference: CVE-2016-7857	https://helpx.ad obe.com/securit y/products/flash -player/apsb16- 37.html	A-ADO- FLASH 181116/13

Mujs
MuJS is a lightweight implementation of the Javascript language in a library. Its primary purpose is

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

to add scripting language.	capability to ot	her prog	grams, but car	ı also be	used as	an exter	isible s	cripting
Denial of Service	11/11/2016	5	Artifex Softw Inc. MuJS bef 5008105780 2ea6eda83ac 25be3ee allo context-depe attackers to c "denial of ser (application attacks by us "malformed break/conting JavaScript" approach, rela a "NULL point dereference" affecting the jscompile.c component. Reference: (ore c0b018 d5598f2 ws endent conduct rvice crash)" ing the labeled aue in	tscript.c	ougs.ghos com/sho egi?id=69	A-AR' MUJS 1811	
			2016-9294					
Cisco								
Hosted Collabora Cisco Hosted Col collaboration pla	llaboration Solu tform for serv	ition (Ho	CS) is a next riders who w	_				
Cross Site Request Forgery	g hosted and ma 03/11/2016	A cross-site r forgery (CSR vulnerability web interface Cisco Hosted Collaboration Mediation Fulfillment application c allow an unauthentica remote attac execute unwactions. More Information: CSCva54241 Known Affec	r) in the e of the ould ated, ker to anted	o.com/s enter/c scoSecu ory/ciso	tools.cisc security/c ontent/Ci rityAdvis co-sa- 26-hcmf	A-CIS HOST 1811		
CV Scoring 0- Scale	1 1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

			Releases: 11.5(Known Fixed Releases: 11.5(0.98000.2 Reference: CV) 2016-6454	16).							
Identity Services Engine Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches. The purpose is to simplify identity management across diverse devices and applications.											
Execute Code; SQL Injection	03/11/2016	4.9	A vulnerability the web framewode of Cisco Identity Service Engine (ISE) coallow an authenticated, remote attacked execute arbitrated SQL commands the database. Moreoff March 1962 March 1962 March 1963 March 1	work es buld r to ry s on lore	o.com/s enter/c		A-CIS IDEN 1811				
Ip Interoperability Cisco IP Interoperability	rability and Col	laboratio	on System (IPICS)			adio dispa	itch op	erations			
and improve resp	03/11/2016	6.6	A vulnerability the command-l interface of the Cisco IP Interoperability Collaboration System (IPICS) could allow an authenticated, l attacker to elev the privilege lev associated with their session. M	in ine y and local rate vel	https://o.com/s enter/c scoSecu ory/cisc	tools.cisc security/c ontent/Ci rityAdvis co-sa- 26-ipics2		G-IPIN 16/17			
CV Scoring O-Scale	1 1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10			

			Information: CSCva38636. Known Affected Releases: 4.10(1). Known Fixed Releases: 5.0(1). Reference: CVE-2016-6430		
Cross Site Scripting	03/11/2016	4.3	A vulnerability in the web framework code of the Cisco IP Interoperability and Collaboration System (IPICS) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. More Information: CSCva47092. Known Affected Releases: 4.10(1). Reference: CVE-2016-6429	https://tools.cisc o.com/security/c enter/content/Ci scoSecurityAdvis ory/cisco-sa- 20161026-ipics1	A-CIS-IPIN 181116/18
and content sha	o conferencing a	eeting S	s you make decisions fa	s-based video, aud	
Execute Code;	03/11/2016	ne collab	oration needs of the m A vulnerability in	https://tools.cisc	A-CIS-
Overflow			Cisco Meeting Server and Meeting App could allow an unauthenticated, remote attacker to execute arbitrary code on an affected system. This vulnerability affects the following products: Cisco Meeting Server releases prior to 2.0.1, Acano Server	o.com/security/c enter/content/Ci scoSecurityAdvis ory/cisco-sa- 20161102-cms	

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

1-2

CV Scoring Scale

0-1

Meeting Serve. Cisco Meeting to meet the col Execute Code;	Serve aborat		s of t		App to 1 Mee rele 1.8. Info CSO Kno Rele Ref 201		prior to ted 1.92.0. EVE- udio, ar	_	communio /tools.cisc	A-CIS	S-
Overflow		,,,			Sessipro par Mee cou una rem exe cod syst vuli the pro Mee rele Rele Ser price 1.9. rele to F Mor CSC Known Rele 1.92	sion Descritocol (SDI) ser of Ciscerting Servella allow an authentical cute arbities on an aftern. This herability following ducts: Ciscerting Server releases 2.0.3 ver releases 1.8.x Release 1.8.x	ription P) co er in ited, ker to rary fected affects co er r to , Acano es 1.9.x ase Server c prior 3.17. ation:	o.com/s enter/c scoSecu ory/cis	security/c ontent/Ci irityAdvis	MEE	
CV Scoring Scale	0-1	1-2	2-	-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Prime Collaboration Provisioning Prime Collaboration Provisioning provides features such as delegation to individual domains, template support for configuring infrastructure instances, advanced batch provisioning and so on. Cross Site Scripting O3/11/2016 Scripting O3/11/2016 A-CIS- Ocom/security/c code of the Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43736 CSCut43736 CSCut43736 CSCut43741 CSCut43741 CSCut43745 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43766 CSCut437				2016-6448		
Prime Home Collaboration Provisioning provides features such as delegation to individual domains, template support for configuring infristructure instances, advanced batch provisioning and so on.	Prime Collaborat	tion Provisionin	a			
CV Scoring O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		-		es features such as	delegation to indivi	dual domains.
Cross Site Scripting O3/11/2016 Scripting O3/11/2016 O4/11/2016 O4/11/2016 O4/11/2016 O4/11/2016 O4/11/201						
Scripting vulnerabilities in the web framework code of the Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43736 CSCut43738 CSCut43741 CSCut43745 CSCut43745 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43766 CSCut43756 CSCut43766				•	*	0
the web framework code of the Cisco Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experimer. Bypass O3/11/2016 Dt. H. 20 2.3 3.4 4.5 5.6 6.7 7.8 8.9 9.410		00/11/2010	1.0	•	. , ,	
CV Scoring O-1 1-2 O-2-3 O-1 O	Scripting				, , , , , , , , , , , , , , , , , , , ,	
Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43741 CSCut43745 CSCut43751 CSCut43756 CSCut43759 CSCut43756 CSCut43766 CSCut43759 CSCut43766 CSCut43759 CSCut43766 CSCut43766 CSCut43759 CSCut43766 CSCut43751 CSCut43766 CSCut43751 CSCut43766 CSCut43751 CSCut43766 C						101110/21
Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43741 CSCut43745 CSCut43745 CSCut43745 CSCut43756 CSCut43756 CSCut43766 Known Affected Releases: 10.6. Reference: CVE-2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an consequence of the web-based graphical user interface (GUI) of Cisco Prime Home could allow an consequence or 7-8 8-9 9-10						
allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43061 CSCut43736 CSCut43736 CSCut43741 CSCut43745 CSCut43745 CSCut43756 CSCut43759 CSCut43759 CSCut43766 Known Affected Releases: 10.6. Reference: CVE-2016-6451 CSCut43766 Known Affected Releases: 10.6. Reference: CVE-2016-6451 CSCut43756 CSCut43750 CSCut43764 CSCut43764 CSCut43764 CSCut43764 CSCut43765 CSCut43765 CSCut43765 CSCut43766 Known Affected Releases: 10.6. Reference: CVE-2016-6451 CSCut43766 Known Affected Releases: 10.6. Reference: CVE-201					_ · ·	
unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43741 CSCut43741 CSCut43745 CSCut43741 CSCut43751 CSCut43756 CSCut43756 CSCut43759 CSCut43756 CSCut43756 CSCut43759 CSCut43764 CSCut43764 CSCut43764 CSCut43764 CSCut43766 Rhown Affected Releases: 10.6. Reference: CVE-2016-6451 Prime Home Toroides visibility into the home network, as also reducing operational costs and improving the subscriber experience: Web-based graphical user interface (GUI) of Cisco Prime Home could allow an https://tools.cisc o.com/security/c enter/content/Cisco Scoecurity/Adviso ory/cisco-sa-1 1-12 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 9-10 1-2				<u> </u>	20101020 pcp	
remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43736 CSCut43741 CSCut43745 CSCut43745 CSCut43759 CSCut43759 CSCut43759 CSCut43764 CSCut43764 CSCut43766 Known Affected Releases: 10.6. Reference: CVE-2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience: Bypass O3/11/2016 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an orycisco-sa- VI Scoring O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
CV Scoring O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 1-12 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 1-2 2-8 5-6 6-7 7-8 8-9 9-10 1-2 2-8 5-6 6-7 7-8 8-9 9-10 1-2 2-8 1-2 1-2 2-8 3-4 4-5 5-6 6-7 7-8 8-9 9-10 1-2 2-8 1-2 1-2 2-8 9-10 1-2 2-8 9-10 1-2 2-8 9-10 1-2						
scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43738 CSCut43741 CSCut43745 CSCut43745 CSCut43745 CSCut43746 CSCut43759 CSCut43759 CSCut43764 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web interface (GUI) of Cisco Prime Home co.com/security/c enter/content/Ci scoSecurityAdvis ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43736 CSCut43741 CSCut43745 CSCut43751 CSCut43756 CSCut43759 CSCut43750 CSCut43764 CSCut43766 CSCut43766 CSCut43760						
user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43738 CSCut43738 CSCut43741 CSCut43745 CSCut43751 CSCut43756 CSCut43759 CSCut43759 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience: Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43738 CSCut43741 CSCut43745 CSCut43751 CSCut43756 CSCut43756 CSCut43756 CSCut43756 CSCut43764 CSCut43766 CSCut4376 CSCut43766 CSC				S		
affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43738 CSCut43741 CSCut43745 CSCut43751 CSCut43756 CSCut43756 CSCut43759 CSCut43756 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an consequently/deight co						
More Information: CSCut43061 CSCut43766 CSCut43738 CSCut43738 CSCut43741 CSCut43745 CSCut43755 CSCut43759 CSCut43766 CSCut43766 CSCut43766 CSCut43766 CSCut43766 CSCut43768 CSCut43768 CSCut43768 CSCut43769 CSCut43766 CSCut43760 CSCu						
CSCut43736 CSCut43736 CSCut43741 CSCut43745 CSCut43756 CSCut43751 CSCut43759 CSCut43759 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				_		
CSCut43736 CSCut43736 CSCut43741 CSCut43745 CSCut43756 CSCut43751 CSCut43759 CSCut43759 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
CSCut43738 CSCut43741 CSCut43745 CSCut43751 CSCut43756 CSCut43756 CSCut43759 CSCut43764 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an converse or conve				CSCut43066		
CSCut43741 CSCut43745 CSCut43748 CSCut43751 CSCut43756 CSCut43756 CSCut43766 CSCut43766 CSCut43766 CSCut43766 CSCut43764 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43736		
CSCut43745 CSCut43748 CSCut43751 CSCut43756 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an Vulnerability in the web-based graphical user interface (GUI) of center/content/Ci scoSecurityAdvis ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43738		
CSCut43748 CSCut43751 CSCut43756 CSCut43759 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an Vulnerability in the web-based graphical user interface (GUI) of cisco Prime Home could allow an CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43741		
CSCut43751 CSCut43756 CSCut43764 CSCut43764 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an viny/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43745		
CSCut43756 CSCut43759 CSCut43764 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an collection ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43748		
CSCut43759 CSCut43764 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43751		
CSCut43764 CSCut43766. Known Affected Releases: 10.6. Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43756		
CSCut43766. Known Affected Releases: 10.6. Reference: CVE-2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43759		
Affected Releases: 10.6. Reference: CVE-2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an Cisco Prime Home or could allow an CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				CSCut43764		
Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass O3/11/2016 O4/10/10/10/10/10/10/10/10/10/10/10/10/10/				CSCut43766. Known		
Reference: CVE- 2016-6451 Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				Affected Releases:		
Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass O3/11/2016 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an vigorial org/cisco-sa- 181116/22 18116/22 181116/22 181116/22 181116/22 181116/22 181116/22 181116/22 181116/22 181116/22 181116/22 181116/22 1						
Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an could allow an could allow an cory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				2016-6451		
solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
improving the subscriber experience. Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						-
Bypass 03/11/2016 10 Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an cory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	_			home network, as al	so reducing operation	onal costs and
web-based graphical user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		_			T	
user interface (GUI) of Cisco Prime Home could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Bypass	03/11/2016		•		
Cisco Prime Home could allow an scoSecurityAdvis ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				9 1		
could allow an ory/cisco-sa- CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					· · · · · · · · · · · · · · · · · · ·	181116/22
CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
				could allow an	ory/cisco-sa-	
Scale		1 1-2 2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10
	Scale					

			acces temp disco LAN o	aging phy s to a VDI orary nnection cable. rence: CV	for of a				
Dotcms									
Dotcms	C.							G. I. G.	
DotCMS is a fre	•	•					•	n (WC	M) for
building/managin	g websites, co	ontent an			web app	NA		A-DO	т
			_	njection	, tha	INA		DOT(
				rability ir Browser :					
								1811	16/24
				s" screen i					
				MS before s remote	3.3.1				
				enticated					
				kers to ex	ocuto				
				ary SQL	ecute				
				nands via	the				
				by param					
				rence: CV					
				-8908	_				
Execute Code; SQL Injection	14/11/2016	6.5	SQL i	njection rability ir		NA		A-DO DOTO	CM
				ent Types ent Types'				1811	16/25
				n in dotCl					
			befor	e 3.3.1 all	ows				
			remo	te authen	ticated				
			attacl	xers to ex	ecute				
			arbiti	ary SQL					
			comn	nands via	the				
			order	by param	eter.				
			Refe	rence: CV	Е-				
				-8907					
Execute Code;	14/11/2016	6.5		njection	_	NA		A-DO	
SQL Injection				rability ir				DOTO	
				Browser				1811	16/26
				s" screen i					
				MS before	5.5.1				
				s remote					
				enticated kers to ex	ecute				
	<u> </u>		actaci	LCIU CO CA	ccate	<u> </u>			
CV Scoring 0-3	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			arbitrary SQL		
			commands via the		
			orderby parameter.		
			Reference: CVE-		
			2016-8906		
Execute Code; SQL Injection	14/11/2016	6.5	SQL injection vulnerability in the	NA	A-DOT- DOTCM
SQL IIIJection			JSONTags servlet in		181116/27
			dotCMS before 3.3.1		101110/27
			allows remote		
			authenticated		
			attackers to execute		
			arbitrary SQL		
			commands via the		
			sort parameter.		
			Reference: CVE-		
			2016-8905		
Execute Code;	14/11/2016	6.5	SQL injection	NA	A-DOT-
SQL Injection			vulnerability in the		DOTCM
			"Site Browser >		181116/28
			Containers pages"		
			screen in dotCMS		
			before 3.3.1 allows		
			remote authenticated		
			attackers to execute		
			arbitrary SQL		
			commands via the		
			orderby parameter. Reference: CVE-		
			2016-8904		
Execute Code;	14/11/2016	6.5	SQL injection	NA	A-DOT-
SQL Injection			vulnerability in the		DOTCM
,			"Site Browser >		181116/29
			Templates pages"		,
			screen in dotCMS		
			before 3.3.1 allows		
			remote authenticated		
			attackers to execute		
			arbitrary SQL		
			commands via the		
			orderby parameter.		
			Reference: CVE- 2016-8903		
Execute Code;	14/11/2016	7.5	SQL injection	NA	A-DOT-
SQL Injection	, , ,		vulnerability in the		DOTCM
, ,	•		· · · · · · · · · · · · · · · · · · ·	•	

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

EMC Avamar Data Sto	re; Avamar Ser	ver Vir	servlet before remote auther attacke arbitra comma sort pa Refere 2016 -	nticated ers to ex ary SQL ands via arameter ence: CV 8902	MS ows ecute the			1811	16/30
EMC Avamar Dat combines Dell E integrated, scalab with multiple ver Avamar data prot	MC certified ha ble, pre-package ndors for hardw	rdware d solut vare, so	and A ion. It e oftware,	vamar b eliminate and sup	ackup as the happort; Av	nd recov ssles and vamar Vi	very softw d complex	vare in ity of v	a fully working
NA	15/11/2016	7.2	EMC A Store (Avama Edition version contain vulner expose server be com malicid	vamar D (ADS) an (AVE) ns 7.3 an a ability the the Ava s to pote npromise ous user ence: CV	ata d d older nat may mar ntially ed by	http://v rityfocu	www.secu s.com/ar /539613	AVAM	_
Exponent Cms Exponent CMS is	•	e Conto	ent Man	ıagemen	t System	, based	on PHP, M	lySQL :	and the
SQL Injection	vork. 03/11/2016	5	Exponent CMS 2.3.9 suffers from a SQL injection vulnerability in "/framework/module s/help/controllers/he lpController.php" affecting the version parameter. Impact is Information		m/expone cms/cor 3c175b	mmit/d5c 60bd26b 85b8f0d2	A-EXI EXPO 1811		
CV Scoring O-Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Disclosure. Reference: CVE- 2016-9135		
SQL Injection	03/11/2016	5	Exponent CMS 2.3.9 suffers from a SQL injection vulnerability in "/expPaginator.php" affecting the order parameter. Impact is Information Disclosure. Reference: CVE-2016-9134	https://github.co m/exponentcms /exponent- cms/commit/d5c 3c175b60bd26b 2b74ec85b8f0d2 544db2c8db	A-EXP- EXPON 181116/33
SQL Injection	03/11/2016	7.5	The Pixidou Image Editor in Exponent CMS prior to v2.3.9 patch 2 could be used to perform an fid SQL Injection. Reference: CVE- 2016-7453	https://github.co m/exponentcms /exponent- cms/commit/c10 92f167cc6c78dc 8bf9bf149946c5 219413df3	A-EXP- EXPON 181116/34
Dirctory Traversal	03/11/2016	5	The Pixidou Image Editor in Exponent CMS prior to v2.3.9 patch 2 could be used to upload a malicious file to any folder on the site via a cpi directory traversal. Reference: CVE- 2016-7452	https://github.co m/exponentcms /exponent- cms/commit/c10 92f167cc6c78dc 8bf9bf149946c5 219413df3	A-EXP- EXPON 181116/35
NA	03/11/2016	7.5	Exponent CMS before 2.3.9 is vulnerable to an attacker uploading a malicious script file using redirection to place the script in an unprotected folder, one allowing script execution. Reference: CVE-2016-7095	http://www.exp onentcms.org/ne ws/security- vulnerability-all- exponent- versions-june- 2016	A-EXP- EXPON 181116/36
SQL Injection	04/11/2016	5	In /framework/modules	https://github.co m/exponentcms	A-EXP- EXPON

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

			/core/controllers/ex pHTMLEditorControll er.php of Exponent CMS 2.4.0, untrusted input is used to construct a table name, and in the selectObject method in mysqli class, table names are wrapped with a character that common filters do not filter, allowing for SQL Injection. Impact is Information Disclosure. Reference: CVE-2016-9184
SQL Injection; Bypass; Gain Information	04/11/2016	5	In /framework/modules /ecommerce/controll ers/orderController.p hp of Exponent CMS 2.4.0, untrusted input is passed into selectObjectsBySql. The method selectObjectsBySql of class mysqli_database uses the injectProof method to prevent SQL injection, but this filter can be bypassed easily: it only sanitizes user input if there are odd numbers of ' or " characters. Impact is Information Disclosure. Reference: CVE- 2016-9183
Bypass	04/11/2016	5	Exponent CMS 2.4 https://github.co A-EXP-uses PHP reflection to call a method of a controller class, and cms/commit/68
CV Scoring O-Scale	1 1-2	2-3	3-4 4-5 5-6 6-7 7-8 8-9 9-10

			then uses the method name to check user permission. But, the method name in PHP reflection is case insensitive, and Exponent CMS permits undefined actions to execute by default, so an attacker can use a capitalized method name to bypass the permission check, e.g., controller=expHTML Editor&action=previe w&editor=ckeditor and controller=expHTML Editor&action=Previe w&editor=ckeditor. An anonymous user will be rejected for the former but can access the latter. Reference: CVE-2016-9182	4d79424f768db8 bb345d5c68aa2a 886239492b	
Execute Code; SQL Injection	11/11/2016		Multiple SQL injection vulnerabilities in the update method in framework/modules/core/controllers/exp RatingController.php in Exponent CMS 2.4.0 allow remote authenticated users to execute arbitrary SQL commands via the (1) content_type or (2) subtype parameter. Reference: CVE-2016-9242 In	https://github.com/exponentcms/exponent-cms/commit/6172f67620ac13fc2f4e9d650c61937d48e9ecb9	A-EXP- EXPON 181116/40
SQL IIIJection	11/11/2010	7.5	framework/modules/ navigation/controller	m/exponentcms /exponent-	EXPON 181116/41
CV Scoring 0- Scale	1 1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			s/navigationCor.php in Expone CMS v2.4.0 or othe parameter "target" of func "DragnDropRefis directly used without any filt which caused Sinjection. The poan be used like /navigation/DropReRank/targ Reference: CVI 2016-9288	ent de la	dffb2e7	nmit/2d eafe4830 4b43787 61ba		
Gain Information	11/11/2016	5	framework/mousers/controller.ph rsController.ph Exponent CMS v2.4.0patch1 doproperly restrict access to user records, which remote attacker ad address information, as demonstrated baddress/show/URI. Reference: CVI 2016-9286	rs/use ry p in / coes not 8 ct / ct / cr / cr / cr / cr / cr / cr /	m/expo /expone cms/cor 8aae660	nmit/e3 :785f08f3 21378caf	EXPO 1811	
Gain Information	11/11/2016	5	framework/modules/ addressbook/controll ers/addressControlle r.php in Exponent CMS v2.4.0 allows remote attackers to read user information via a modified id number, as demonstrated by address/edit/id/1, related to an "addresses, countries, and regions" issue. Reference: CVE-		m/expo /expone cms/cor ed1e82f	nmit/9ee ъ9e6d0d 10672df4		
CV Scoring O-3	1 1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

			2016-9285		
Gain Information	11/11/2016	5	getUsersByJSON in framework/modules/ users/controllers/use rsController.php in Exponent CMS v2.4.0 allows remote attackers to read user information via users/getUsersByJSO N/sort/ and a trailing string. Reference: CVE-2016-9284	https://github.co m/exponentcms /exponent- cms/commit/e7 b6856ac384bf2b 8ea7761a1e46d6 e4186d36f4	A-EXP- EXPON 181116/44
SQL Injection	11/11/2016	5	SQL Injection in framework/core/sub systems/expRouter.p hp in Exponent CMS v2.4.0 allows remote attackers to read database information via address/addContentT oSearch/id/ and a trailing string, related to a "sef URL" issue. Reference: CVE-2016-9283	https://github.com/exponentcms/exponent-cms/commit/559792be727f4e731bfcb3935f5beec7749e9ce9	A-EXP- EXPON 181116/45
SQL Injection	11/11/2016	5	SQL Injection in framework/modules/ search/controllers/se archController.php in Exponent CMS v2.4.0 allows remote attackers to read database information via action=search&modul e=search with the search_string parameter. Reference: CVE-2016-9282	https://github.co m/exponentcms /exponent- cms/commit/e8 3721a5b9fcc88e 1141a8fb29c3d1 bd522257c1	A-EXP- EXPON 181116/46
Denial of Service; SQL	11/11/2016	6.4	A Blind SQL Injection Vulnerability in	https://exponent cms.lighthouseap	A-EXP- EXPON

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

Injection			Exponent CMS through 2.4.0, with the rerank array parameter, can lead to site database information disclosure and denial of service. Reference: CVE- 2016-9272	p.com/projects/ 61783/tickets/1 394-blind-sql- injection- vulnerability-in- exponent-cms- 240-4	181116/47
SQL Injection Git For Windows	15/11/2016	7.5	In /framework/modules /notfound/controller s/notfoundController. php of Exponent CMS 2.4.0 patch1, untrusted input is passed into getSearchResults. The method getSearchResults is defined in the search model with the parameter '\$term' used directly in SQL. Impact is a SQL injection. Reference: CVE- 2016-9287	https://github.com/exponentcms/exponent-cms/commit/4327ea96b3de89440693e06d03038121aa1fdcea	A-EXP- EXPON 181116/48
	SProject				
			ntweight, native set of too appropriate user interfa		
Gain Privileges	11/11/2016	4.4	Untrusted search path vulnerability in Git 1.x for Windows allows local users to gain privileges via a Trojan horse git.exe file in the current working directory. NOTE: 2.x is unaffected. Reference: CVE-2016-9274	NA	A-GIT-GITF 181116/49

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

1-2

CV Scoring Scale

0-1

Gitlab Gitlab Gitlab is a free software, which provides Git repository management, code reviews, issue tracking, activity feeds and wikis. 03/11/2016 Gain 4 GitLab versions https://about.gitl A-GITab.com/2016/11 Information 8.9.x and above GITLA-contain a critical /02/cve-2016-181116/50 9086-patches/ security flaw in the "import/export project" feature of GitLab. Added in GitLab 8.9, this feature allows a user to export and then re-import their projects as tape archive files (tar). All GitLab versions prior to 8.13.0 restricted this feature to administrators only. Starting with version 8.13.0 this feature was made available to all users. This feature did not properly check for symbolic links in userprovided archives and therefore it was possible for an authenticated user to retrieve the contents of any file accessible to the GitLab service account. This included sensitive files such as those that contain secret tokens used by the GitLab service to authenticate users. **CV** Scoring 0-1 1-2 2-3 3-4 4-5 **5-6** 6-7 7-8 8-9 9-10 Scale

ISC			vers thro 8.12 8.12 thro 8.10 thro affe Ref	Lab CE and sions 8.13 bugh 8.13 2.0 through 8.11 0.0 through 8.9.1 cted. erence: C	3.0 .2, gh .10, gh 8.9.0				
Bind									
BIND is open sour	rce software	that imp	olements	the Dom	ain Nan	ne System	n (DNS) pr	rotocols	for the
Internet. Denial of Service	02/11/201	.6 5	9.x 9.10 P4, before allo attanden (ass and via in the sectorespondent resources reconsectores	ned in ISC before 9.9 0.x before and 9.11.0 ore 9.11.0 ws remot ckers to c ial of serv sertion fai daemon a DNAME he answer ion of a conse to a ursive que ted to db. olver.c. erence: 0	9.9-P4, 9.10.4- x -P1 ee cause a vice lure exit) record r	https://g/articl 01434	/kb.isc.or e/AA-		-BIND 16/51
Joomla									
Joomla! Joomla! is the moh	ile-ready an	d user-fr	iendly w	ay to buil	d vour w	rehsite It	is free and	d onen s	source
NA	04/11/201		The in the Use tion con p in	Ily way to build your w The register method in the UsersModelRegistra tion class in controllers/user.ph p in the Users component in			github.co nla/jooml mmit/bae 8c87848 571e4945 fdcf	A-J00 J00M 1811)-
CV Scoring 0-3 Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

					_						
Gain Privileges	04	·/11/201	16	7.5	wh has allo atta use level che Use correct Ref 20 The in t Use tion correct pir correct Joo allo atta pri level use dat reg Ref	mla! beforen registration der accounts eraging fatter the Alle er Registrating. ference: Compare the ers Model Register in the Users i	ation abled, se create s by ilure to ow ation a correct red a site.	m/joom a- cms/co 1d4393	github.co nla/jooml mmit/bae 8c87848 571e4945 fdcf	JOOM 1811	
Microfocus Rumba RUMBA software	mal	kes it eas	sy to	conr	nect to a	and use in	formatic	n on IRN	1 mainfra	me IRM	1 iSeries
(AS/400), UNIX, optimal perform	Hew	lett-Pack	ard,	and '	VAX sys	tems. Mic	ro Focus	ss modula			
Execute Code; Overflow		3/11/201		7.5	Sta ove sen rec con Mic 9.4 be	ck buffer erflow in the deexe and eive.exe ero Focus hand earlied used by loackers or eckers able	he of Rumba er could cal	https:// ploit-	www.ex/exploits/	A-MI RUM 1811	
CV Scoring ()-1	1-2	2	-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Scale

			these execu Refer	argume binarie te code ence: (s to				
Microsoft								•	
Edge Edge is a smaller services.	, more stream	nlined br	owser l	ouilt o	n Web s	standards	and des	igned f	for Web
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	engin Edge a attack arbitr cause service corru- crafte "Scrip Memo Vulne differe vulne CVE-2 CVE-2 CVE-2 CVE-2 CVE-2 Refer	cript scree in Mice allows in Mice allows in General Control of the Control of th	crosoft cemote execute le or al of nory via a site, aka igine cuption c," a than 200, 201, 202, 203, 208, 240, 6-	icrosoft us/secu	technet.m .com/en- urity/bull s16-129	EDGI	
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	JavaSo engin Edge a attack arbitr cause servic corru	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine		icrosoft us/secu	technet.m .com/en- urity/bull s16-129	A-MI EDGI 1811	
CV Scoring Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Vulndiffe vuln CVE CVE CVE CVE CVE CVE And 724	nory Correct of the c	than 200, 201, 202, 203, 208, 240,				
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Java enging Edge attains arbition causes served correct of the	Chakra Script sc	erosoft remote execute e or il of nory via a site, aka gine ruption ," a than 200, 201, 202, 203, 208, 242, 6-	icrosoft	echnet.m .com/en- urity/bull s16-129	A-MI EDGH 1811	
NA	10/11/2016	2.6	allov atta web craf "Mid	Microsoft Edge allows remote attackers to spoof web content via a crafted web site, aka "Microsoft Edge Spoofing			technet.m .com/en- arity/bull s16-129	A-MI EDGI 1811	
CV Scoring 0-	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Wuln onchiliter "		
			Vulnerability." Reference: CVE-		
			2016-7209		
Denial of	10/11/2016	7.6	The Chakra	http://technet.m	A-MIC-
Service; Execute	10/11/2010	7.0	JavaScript scripting	icrosoft.com/en-	EDGE
Code; Overflow;			engine in Microsoft	us/security/bull	181116/59
Memory			Edge allows remote	etin/ms16-129	101110/37
Corruption			attackers to execute	ctiii/111310 127	
dorruption			arbitrary code or		
			cause a denial of		
			service (memory		
			corruption) via a		
			crafted web site, aka		
			"Scripting Engine		
			Memory Corruption		
			Vulnerability," a		
			different		
			vulnerability than		
			CVE-2016-7200,		
			CVE-2016-7201,		
			CVE-2016-7202,		
			CVE-2016-7203,		
			CVE-2016-7240,		
			CVE-2016-7242,		
			and CVE-2016-		
			7243.		
			Reference: CVE- 2016-7208		
Gain Information	10/11/2016	2.6	Microsoft Edge	http://technet.m	A-MIC-
	10/11/2010	2.0	allows remote	icrosoft.com/en-	EDGE
			attackers to access	us/security/bull	181116/60
			arbitrary "My	etin/ms16-129	101110,00
			Documents" files via		
			a crafted web site,		
			aka "Microsoft Edge		
			Information		
			Disclosure		
			Vulnerability."		
			Reference: CVE-		
			2016-7204		
Denial of	10/11/2016	7.6	The Chakra	http://technet.m	A-MIC-
Service; Execute			JavaScript scripting	icrosoft.com/en-	EDGE
Code; Overflow;			engine in Microsoft	us/security/bull	181116/61
Memory			Edge allows remote	etin/ms16-129	
Corruption			attackers to execute		

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

			arbitrary code or		
			cause a denial of		
			service (memory		
			corruption) via a		
			crafted web site, aka		
			"Scripting Engine		
			Memory Corruption		
			Vulnerability," a different		
			vulnerability than		
			CVE-2016-7200,		
			CVE-2016-7201,		
			CVE-2016-7202,		
			CVE-2016-7208,		
			CVE-2016-7240,		
			CVE-2016-7242, and CVE-2016-		
			7243.		
			Reference: CVE-		
Denial of	10/11/2016	7.6	2016-7203 The Chakra	http://tochnot.m	A-MIC-
Service; Execute	10/11/2016	7.0	JavaScript scripting	http://technet.m icrosoft.com/en-	EDGE
Code; Overflow;			engine in Microsoft	us/security/bull	181116/62
Memory			Edge allows remote	etin/ms16-129	101110/02
Corruption			attackers to execute	ctin/m310 12)	
Corruption			arbitrary code or		
			cause a denial of		
			service (memory		
			corruption) via a		
			crafted web site, aka		
			"Scripting Engine		
			Memory Corruption		
			Vulnerability," a		
			different		
			vulnerability than		
			CVE-2016-7200,		
			CVE-2016-7201,		
			CVE-2016-7203,		
			CVE-2016-7208,		
			CVE-2016-7240,		
			CVE-2016-7242,		
			and CVE-2016-		
			7243.		
			Reference: CVE-		
			2016-7202		
	<u> </u>		<u> </u>	<u> </u>	<u> </u>

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

Denial of	10/11/2016	7.6	The Chakra	http://technet.m	A-MIC-		
Service; Execute	10/11/2010	7.0	JavaScript scripting	icrosoft.com/en-	EDGE		
Code; Overflow;			engine in Microsoft	us/security/bull	181116/63		
Memory			Edge allows remote	etin/ms16-129	101110/03		
Corruption			attackers to execute	cem/m310 12 /			
Gorraption			arbitrary code or				
			cause a denial of				
			service (memory				
			corruption) via a				
			crafted web site, aka				
			"Scripting Engine				
			Memory Corruption				
			Vulnerability," a				
			different				
			vulnerability than				
			CVE-2016-7200,				
			CVE-2016-7202,				
			CVE-2016-7203,				
			CVE-2016-7208,				
			CVE-2016-7240,				
			CVE-2016-7242,				
			and CVE-2016-				
			7243.				
			Reference: CVE-				
			2016-7201				
Denial of	10/11/2016	7.6	The Chakra	http://technet.m	A-MIC-		
Service; Execute	10/11/2016	7.6	The Chakra JavaScript scripting	icrosoft.com/en-	EDGE		
Service; Execute Code; Overflow;	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft	icrosoft.com/en- us/security/bull			
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote	icrosoft.com/en-	EDGE		
Service; Execute Code; Overflow;	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201,	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7202,	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201,	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7203,	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7203, CVE-2016-7208,	icrosoft.com/en- us/security/bull	EDGE		
Service; Execute Code; Overflow; Memory Corruption			The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7240, CVE-2016-7242,	icrosoft.com/en- us/security/bull etin/ms16-129	EDGE 181116/64		
Service; Execute Code; Overflow; Memory		7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240,	icrosoft.com/en- us/security/bull	EDGE		

					72 ⁴ Re f	l CVE-201 43. ference: C 16-7200					
Edge; Internet Edge is a sm services; Internet Microsoft Wit	naller, 1 ernet Ex	nore stre xplorer is	a w	eb br	rowser					_	
Bypass; Gain Information	1	0/11/201	16	2.6	Mic Exp 11 Edg atta the Pol sen sta via site Bro Info Dis Vul Rei 20		rough soft emote bypass gin dow-tion web rosoft	NA			1; 16/65
Denial of Service; Exec Code; Overflo Memory Corruption	cute ow;	0/11/201		7.6	Exp 11 Edg atta arb cau ser cor cra "M: Me Vul diff vul CVI Rei 20	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7195. Reference: CVE- 2016-7198		NA			16/66
Denial of Service; Exec		0/11/201	16	7.6		Microsoft Internet NA Explorer 10 and 11			A-MIC- EDGE		
CV Scoring	0-1	1-2	2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Scale

Code; Overflow; Memory				Microsof w remote	_			1811	16/67
Corruption				ckers to e					
•			arb	itrary cod	e or				
			cau	se a denia	l of				
			serv	rice (mem	ory				
			cor	ruption) v	ia a				
			craf	ted web s	ite, aka				
			"Mi	crosoft Br	owser				
				nory Corr	•				
				nerability					
				erence: C	VE-				
				6-7196					_
Denial of	10/11/201	6 7.6	_	rosoft Inte		NA		A-MIO	
Service; Execute			_	lorer 9 th	_			EDGE	•
Code; Overflow;				and Micro				1811	16/68
Memory			_	e allow re					
Corruption				ckers to e					
				itrary cod					
				se a denia					
				ice (mem	-				
				ruption) v ted web s					
				crosoft Br	•				
				nory Corr					
				nerability,	_				
				erent	, α				
			_	nerability	than				
				E-2016-71					
			Ref	erence: C	VE-				
			201	6-7195					
Excel For Mac; O	ffice; Office	Compat	ibility P	ack; Offic	ce Web	Apps; Sh	arepoint	Server	; Word;
Word Automation							-		
MS Office offers v						•			
platforms; Microso		•		-	•				
and iOS. It feature			ng tools	, pivot tal	oles, and	a macro	o progran	nming la	anguage
called Visual Basic Denial of	* *		Mia	rosoft Wo	rd	http://	ochnot m	A-MI	2
Service; Gain	10/11/201	4.5		7, Office 2			echnet.m .com/en-	EXCE	
Information				, Word 20			rity/bull		ւ 16/69
imoi manon				, Word 20 , Word foi		etin/ms		1011	10/09
				1, Excel fo			10 100		
				1, Excel id					
				ce Compa	•				
			UIII	Joinpu		ī			
			Pac	•					
			Pac	k SP3, Wo					

Scale

			on S Servand Appallo atta sens info pro caus servand doc "Mi Info Diso Vulta Ref 201	omation ScharePoint ver 2013 ScharePoint ver 2013 Schare Vers 2010 Schare vers to constitute the constitute of the const	ot SP1, eb P2 obtain From ory or of- of- via a ca ffice				
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	200 SP2 SP2 SP1 SP1 201 201 for : Con SP3 Aut on S Serv Wor Serv Sha 201 Wel and App SP1 atta arbi	rosoft Wo 7, Office 2 , Word 20 , Word 20 , Word fo 1, Excel fo 1, Word 2 Mac, Office patibility Word omation S GharePoint ver 2010 fo cd Autom vices on rePoint Se 3 SP1, Office Wo s Server 2 allow rer ckers to e trary cod ted Office	2010 010 013 013 RT or Mac 0016 0e 0 Pack Services 0t SP2, ation erver fice 10 SP2, eb 2013 note execute e via a	icrosoft us/secu	echnet.m .com/en- rity/bull s16-133	A-MI EXCE 1811	
CV Scoring 0-	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7234		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, Excel for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7235	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133	A-MIC- EXCEL 181116/71
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Excel 2007 SP3, Excel for Mac 2011, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7231	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133	A-MIC- EXCEL 181116/72
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133	A-MIC- EXCEL 181116/73

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

CV Scoring 0-3 Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Mic 200 201 201 201 201 201 Mac Con SP3 atta arb:	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a		icrosoft us/secu	technet.m com/en- urity/bull s16-133	A-MI EXCE 1811	_
Execute Code; Overflow; Memory Corruption	10/11/2016	5 9.3	exectod Offication and Offication of Section 1998 and Offication 1	note attack cute arbit e via a cra ce docum "Microso ce Memor ruption nerability erence: O L6-7229 rosoft Exc 7 SP3, Ex 3 SP1, Ex 3 SP1, Ex 3 SP1, Ex 3 SP1, Ex 3 SP1, Ex 1, Excel 2 c, and Offinatibility allow rer sckers to exite of the office ument, all crosoft Office umerability	rary Ifted ent, ft Ty I' I' IVE- Cel cel cel cel or Mac 016 for ce v Pack note execute e via a fice ruption ."	icrosoft us/secu	technet.m c.com/en- rrity/bull s16-133	A-MI EXCE 1811	
			Mad Con SP3	1, Excel 2 c, Office npatibility , and Exce wer allow	v Pack el				

Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Over		T				1
Execute Code; Overflow; Memory Corruption Corruption Pullifor Service Page 10/11/2016 Execute Code; Overflow; Memory Corruption Corruption Execute Code; Overflow; Memory Corruption Pulliform SharePoint Server Page 2016 F243 Page 2016 for Mac 2011, Excel Point Server Page 2010 SP2, Excel for Mac 2011, Excel Point Server Page 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Page 2013 SP1, Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office document, aka "Mic						
Execute Code; Overflow; Memory Corruption Vulnerability." Reference: CVE-2016-7213 Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Corruption Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Corruption Corruption Execute Code; Overflow; Memory Execute arbitrary Code via a crafted Office document, aka "Microsoft Office docu				•		
Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Exec Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office 2013 SP1, office 2016 allow remote attackers to execute arbitrary code via a crafted office document, aka "Microsoft office 2016 allow remote attackers to execute arbitrary code via a crafted office document, aka "Microsoft office 2016 allow remote attackers to execute arbitrary code via a crafted office document, aka "Microsoft office document, aka				"Microsoft Office		
Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Excel Services on SharePoint Server 2010 SP2, Excel for Mac 2011, Excel 2016 for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7236 Execute Code; Overflow; Memory Corruption Corruption Execute Code; Overflow; Memory Corruption Corruption Execute Code; Overflow; Memory Execute Code; Overflow; Memory Corruption Execute Code; Overf				Memory Corruption		
Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Excel Services on SharePoint Server 2010 SP2, Excel for Mac 2011, Excel 2016 for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7236 Execute Code; Overflow; Memory Corruption Corruption Execute Code; Overflow; Memory Corruption Corruption Execute Code; Overflow; Memory Execute Code; Overflow; Memory Corruption Execute Code; Overf				Vulnerability."		
Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Memory Corruption Vulnerability." Reference: CVE-2013 SP2, Office 2013 SP2, Office 2013 SP1, Office 2014 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office 400 with a crafted Office document, aka "Microsoft Office 400 with a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3				_		
Execute Code; Overflow; Memory Corruption Execute Code; Overflow; M						
Overflow; Memory Corruption EXCEL- Mac 2011, Excel 2016 for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office Memory Corruption Vulnerability." Reference: CVE- 2013 SP2, Excel for Mac 2011, Excel 2016 SP2, Excel for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office Memory Corruption Vulnerability." Reference: CVE- 2016-7236 Execute Code; Overflow; Memory Corruption Vulnerability. Reference: CVE- 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to execute arbitrary code via a crafted Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133 A-MIC- OFFIC- 181116/78	Execute Code:	10/11/2016	9.3		httn://technet.m	A-MIC-
Memory Corruption Mac 2011, Excel 2016 for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2013 SP1, office 2014 Allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of etin/ms16-133 181116/76 181116/76 181116/76 181116/76 181116/76 A-MIC- OFFIC- 181116/78	· ·	10/11/2010	7.5		2	
Corruption 2016 for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office Memory Corruption Vulnerability." Reference: CVE-2013 SP1, Office 2013 SP1, office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016 Allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to execute arbitrary code via a crafted Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of vulnerability. The proposition of	•			· ·	,	
Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7236 Execute Code; Overflow; Memory Corruption Execute Code; Overflow; Page 10/11/2016 Execute Code; Overflow; Page 10/	_			· ·	, , ,	181110/76
SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7236 Microsoft Office 2007 SP3, Office 2013 SP1, office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allow remote attackers to execute arbitrary coffice document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allow remote attackers to cause a denial of http://technet.m icrosoft.com/en- icr	Corruption			•	etin/ms16-133	
Execute Code; Overflow; Memory Corruption Corruption Corruption Corruption Execute Code; Overflow; Memory Corruption Corruption Corruption Corruption Execute Code; Overflow; Memory Corruption Corruption Fig. 4.3 Microsoft Office Covering Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of						
remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7236 Execute Code; Overflow; Memory Corruption Corruption Corruption Denial of Service Population Temote attackers to execute arbitrary code via a crafted Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service Total remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 A-MIC-OFFIC-181116/77 A-MIC-OFFIC-181116/78				SharePoint Server		
execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7236 Execute Code; Overflow; Memory Corruption Veriflow: Memory Corruption Corruption Execute Code; Overflow; Memory Corruption Corruption Denial of Service Denial of Service Total and the service of the service				2010 SP2 allow		
Execute Code; Orruption Office Memory Corruption Vulnerability." Reference: CVE- 2016-7236 Execute Code; Overflow; Memory Corruption Vulnerability." Reference: CVE- 2010 SP2, Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office do				remote attackers to		
Execute Code; Orruption Office Memory Corruption Vulnerability." Reference: CVE- 2016-7236 Execute Code; Overflow; Memory Corruption Vulnerability." Reference: CVE- 2010 SP2, Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office do				execute arbitrary		
Execute Code; Overflow; Memory Corruption Vulnerability." Reference: CVE- 2016-7236 Execute Code; Overflow; Memory Corruption Vulnerability." Reference: CVE- 2010 SP2, Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office Memory Corruption Denial of Service 10/11/2016 4.3 Denial of Service 10/11/2016 A-MIC- 0FFIC 181116/77 A-MIC- 0FFIC 181116/77 A-MIC- 0FFIC 181116/77 A-MIC- 0FFIC 181116/78 A-MIC- 0FFIC 181116/78 A-MIC- 0FFIC 181116/78				_		
aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7236 Execute Code; Overflow; Memory Corruption Vunerability." Reference: CVE-2010 SP2, Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2016 allow remote attackers to execute arbitrary code via a crafted Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of http://technet.m icrosoft.com/enus/security/bull etin/ms16-133						
Execute Code; Overflow; Memory Corruption Vulnerability." Reference: CVE- 2016-7236 Execute Code; Overflow; Memory Corruption Vourption 9.3 Microsoft Office 2007 SP3, Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of http://technet.m icrosoft.com/en-us/security/bull etin/ms16-133 A-MIC-OFFIC 181116/78				•		
Execute Code; Overflow; Memory Corruption Corruption Vulnerability." Reference: CVE-2016-7236 Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Corruption Vulnerability." Reference: CVE-2016 SP2, Office 2016 Allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Mitp://technet.m icrosoft.com/enus/security/bull etin/ms16-133						
Execute Code; Overflow; Memory Corruption Denial of Service Denial of Service Tight Spring and S				_		
Execute Code; Overflow; Memory Corruption Parish and Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office Memory Corruption Vulnerability." Denial of Service T0/11/2016 A.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Service T0/11/2016 A.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Service T0/11/2016 A.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Service T0/11/2016 A.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Service T0/11/2016 Service T0/11/2016 A.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Service T0/11/2016 Service T0/11/2016 A.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Service T0/11/2016 Service T				-		
Execute Code; Overflow; Memory Corruption Parish and Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Denial of Service Denial of Service 10/11/2016 A.3 Microsoft Office 2007 SP3 allows remote attackers to execute a chail of cause a denial of cause a				_		
Execute Code; Overflow; Overflow; Memory Corruption Denial of Service Denial of Service Denial of Service Denial of Service Overflow; Memory Corruption 10/11/2016 10/11/2016 9.3 Microsoft Office 2007 SP3, Office 2013 SP1, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2016 Memory Corruption Vulnerability." Reference: CVE-2016-7245 A-MIC-OFFIC-181116/78 A-MIC-OFFIC-181116/78						
Overflow; Memory Corruption 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133 OFFIC 181116/77 181116/77 A-MIC- OFFIC 181116/78						
Memory Corruption 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133 181116/77 181116/77 A-MIC- OFFIC 181116/78	·	10/11/2016	9.3			
Corruption 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133	Overflow;			2007 SP3, Office	icrosoft.com/en-	OFFIC
Denial of Service Denial of Service 10/11/2016 Denial of Service 10/11/2016 Denial of Service 10/11/2016 10/11/2016 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Microsoft Office 2007 SP3 allows icrosoft.com/enicrosoft.com/enicrosoft.com/enus/security/bull etin/ms16-133 A-MIC-OFFIC181116/78	Memory			2010 SP2, Office	us/security/bull	181116/77
Denial of Service Denial of Service 10/11/2016 Denial of Service 10/11/2016 Denial of Service 10/11/2016 10/11/2016 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Microsoft Office 2007 SP3 allows icrosoft.com/enicrosoft.com/enicrosoft.com/enus/security/bull etin/ms16-133 A-MIC-OFFIC181116/78	Corruption			2013 SP1, Office	etin/ms16-133	
Denial of Service 10/11/2016 Denial of Service 10/11/2016 Denial of Service 10/11/2016 Denial of Service 10/11/2016 10/11/2016 A-MIC- 2007 SP3 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of Nttp://technet.m icrosoft.com/en- us/security/bull etin/ms16-133	1			·	,	
remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of http://technet.m icrosoft.com/enus/security/bull etin/ms16-133 A-MIC-181116/78						
execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE-2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office http://technet.m icrosoft.com/en-remote attackers to cause a denial of etin/ms16-133 A-MIC-181116/78						
code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of wind via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." A-MIC- OFFIC 181116/78						
Denial of Service Denial of Service 10/11/2016 A-MIC- 2007 SP3 allows remote attackers to cause a denial of Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of A-MIC- OFFIC 181116/78				•		
aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of windows in the property of the prop						
Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of etin/ms16-133 Office 2016/78 Page 18/11/2016 Page 18/1				·		
Corruption Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office http://technet.m icrosoft.com/en- us/security/bull 181116/78 cause a denial of etin/ms16-133						
Vulnerability." Reference: CVE- 2016-7245 Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows icrosoft.com/en- us/security/bull tein/ms16-133 181116/78				-		
Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of etin/ms16-133 Reference: CVE-2016-7245 Microsoft Office 10/11/2016 A-MIC-0FFIC18/1116/78 Reference: CVE-2016-7245 Microsoft Office 10/11/2016 A-MIC-18/1116/78				*		
Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of etin/ms16-133 A-MIC-131				Vulnerability."		
Denial of Service 10/11/2016 4.3 Microsoft Office 2007 SP3 allows remote attackers to cause a denial of etin/ms16-133 A-MIC-OFFIC181116/78				Reference: CVE-		
2007 SP3 allows icrosoft.com/en-us/security/bull etin/ms16-133 OFFIC				2016-7245		
2007 SP3 allows icrosoft.com/en-us/security/bull etin/ms16-133 OFFIC	Denial of Service	10/11/2016	4.3	Microsoft Office	http://technet.m	A-MIC-
remote attackers to cause a denial of us/security/bull etin/ms16-133					* ' '	
cause a denial of etin/ms16-133					-	
, , , , , , , , , , , , , , , , , , ,						
service (apprication						
		1		service (application	<u> </u>	<u> </u>

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

			hang) via a crafted Office document, aka "Microsoft Office Denial of Service Vulnerability." Reference: CVE- 2016-7244		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft PowerPoint 2010 SP2, PowerPoint Viewer, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7230	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133	A-MIC- OFFIC 181116/79
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Reference: CVE- 2016-7232	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-133	A-MIC- OFFIC 181116/80

SQL Server

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications, which may run either on the same computer or on another computer across a network (including the Internet).

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

Gain Privileges	10/11/201	6 6.5	201 doe per uns whi rem auth to g unk aka Eng Priv Vul Ref 201 Mic Ser not per uns whi rem auth to g unk aka Eng	2014 SP2, and 2016 does not properly perform a cast of an unspecified pointer, which allows remote authenticated users to gain privileges via unknown vectors, aka "SQL RDBMS Engine Elevation of Privilege Vulnerability." Reference: CVE-2016-7250		us/secu etin/ms http://t icrosoft	echnet.m .com/en- rity/bull	A-MI0 S	16/81 C-SQL 16/82
			Vul Ref	nerability erence: 0 16-7249					
Moinmo				7217					
Moinmoin									
MoinMoin is a wik								ki engine	e. Its
name is a play on						1			AT.
Cross Site Scripting	10/11/201	6 4.3	allo atta "Jav inje usii crea rela	MoinMoin 1.9.8 allows remote attackers to conduct "JavaScript injection" attacks by using the "page creation" approach, related to a "Cross Site Scripting (XSS)"			www.cur n/blog/a log/Moin 98-XSS- il	MOIN	
CV Scoring O-Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

					act (vi co	ue affectin ion=Attacl a page nan nponent. ference: (nFile ne)				
Cross Site Scripting	10/2	11/201	6	4.3	Mo all att "Ja inj usi cre UR rel Sit iss act alc (vi con	ninMoin 1.9 ows remote ackers to covaScript ection" attempted in a rection or contact and the second in a rection of the second in a rection of the second in a page name in ponent. ference: Common of the second in a page name in the second in a page name in the second in the seco	e conduct acks by ge cafted ch, Cross (XSS)" g the alog&dinent ne)	esec.cor		MOIN	
Moodle											
Moodle Moodle is free a distributed under							anagem	ent syste	em writte	n in P	HP and
Cross Site Scripting	04/2	11/201	6	4.3	Cre (XX) in be rei inj scr the s_a d, s_a off s_a er Re 20	Cross-site scripting (XSS) vulnerabilities in Moodle CMS on or before 3.1.2 allow remote attackers to inject arbitrary web script or HTML via the s_additionalhtmlhea d, s_additionalhtmltop ofbody, and s_additionalhtmlfoot er parameters. Reference: CVE-		ormsect /files/1 oodle-C Cross-S Scriptin Upload.	g-File- html		DL 16/85
Execute Code	04/2	11/201	6	6.5		Unrestricted file upload vulnerability			https://packetst ormsecurity.com		00- DL
CV Scoring O-Scale	1	1-2	2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Execute Code	04/11/201	6 6.	.5	externing Mallov authors to externing Reference unspection the files manning Mallov authors executed acceptable with the execution of the exec	te double nsion sur 'image" n codle 3.1 ws remote ecute arle by uploa with an existing it voccified verence: Code and "file ager" mote codle 3.1 ws remote enticated with an existing it voccified verence: Code and "file ager" mote codle 3.1 ws remote enticated with an existing it voccified verence: Code and "file ager" mote codle 3.1 ws remote enticated with an existing it voccified verence: Code and "file ager" mote enticated execute arle by uploa with an existing it voccified verence: Code and the code and	oport in nodule2 e dusers bitrary ading a d then ia ectors. EVE- file rability course e dules2 e dusers bitrary ading a d then ia ectors.	oodle-C Cross-Si Scriptin Upload. https:// ormsect /files/1	g-File- html packetst urity.com 39466/M MS-3.1.2- ite- g-File-	A-MC MOO! 1811	
				201	6-9186					
Novell	orvor 11. O	non Er	ntoun	ico C	oruge 201	15				
Open Enterprise Se Open Enterprise Se SUSE Linux Enterpr	erver brings	the in	-				and prin	t services	onto th	ne latest
NA NA	15/11/20		6.4	Vulnerability in Novell Open Enterprise Server (OES2015 SP1 before Scheduled Maintenance Update 10992, OES2015 before Scheduled Maintenance Update			novell.c	lownload om/Dow uildid=s9 3KU~	OPEN	
CV Scoring 0-1 Scale	1-2	2-3		3-4	4-5	5-6	6-7	7-8	8-9	9-10

				beformal 109 beformal 109 authorized performal accommod Ref	90, OES1 ore Sched ntenance 91, OES1 ore Sched ntenance 89) migh nenticated form uthorized ess and dification. erence: 0	uled Update 1 SP2 uled Update t allow d kers to				
Nvidia										
Geforce Experience NA	e									
Denial of Service; Overflow	08/11/20	16 7	7.2	Qua GeF NVI Exp befo 2.11 befo con vuli keri (nvi allo cau ove spec exec lead of si esca priv Ref	the NVID adro, NVS, orce proceuted are GFE and a stains a merability mel mode streamkm wing a usually craftcutable paling to a dervice or alation of vileges.	and lucts, rce 340 and R375 an	thelp.co	nvidia.cus om/app/a /detail/a_ 7	A-NV GEFC 1811	
Execute Code	08/11/20	16 7	'.2	For the NVIDIA Quadro, NVS, and GeForce products, GFE GameStream			thelp.com/app/a			I-)R 16/90
CV Scoring 0-1 Scale	1-2	2-3		3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring 0-1 Scale	1-2	2-3	3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
NA	08/11/2016	6.4	9	Windows gradrivers. Reference: C 2016-4961 For the NVID Quadro, NVS, GeForce proof the NVIDIA NVStreamKM service comp is improperly validating use supplied data	thelp.co nswers id/4213		GEF0 1811	PR 16/92	
Denial of Service	08/11/2016	4.	9	a vulnerable installation constallation constallation constalled malicic code to execut the system at system/user privilege lever CVE-2016-58 is for the NVT Plugin unquo service path. Reference: Constalled Transfer Constalled	service an ous ite on the el. The ES2 ID Tray ited EVE- IA and lucts, of the IS.sys sed a vice (blue	thelp.co	nvidia.cus om/app/a /detail/a_ 3	GEFO	
				and NVTray I unquoted ser path vulneral are examples unquoted ser path vulneral Windows. A successful ex	vice bilities of the vice bility in				

			enti an e priv	ough its All by points of elevation of vilege. erence: C	causing of				
Execute Code	08/11/201	6 7.2	For Qua GeF GFF and unqual path wire successive ena cod the system of the Gan unqual transfer of the system of the	Reference: CVE-2016-4960 For the NVIDIA Quadro, NVS, and GeForce products, GFE GameStream and NVTray Plugin unquoted service path vulnerabilities are examples of the unquoted service path vulnerability in Windows. A successful exploit of a vulnerable service installation can enable malicious code to execute on the system at the system/user privilege level. The CVE-2016-3161 ID is for the GameStream unquoted service path.		thelp.co	nvidia.cus om/app/a /detail/a_ }	GEFO	
Gpu Driver Nvidia GPU-acceler CPU to accelerate d	_	_	use o	of a graph	_	_	nit (GPU)	togethe	r with a
Denial of Service	08/11/201		For Qua GeF NVI GPU R34 and 375 vuli	the NVID dro, NVS, orce prod DIA Wind J Display I 0 before 3 R375 bef 1.63 containerability nel mode	IA and lucts, ows Driver 342.00 ore ins a in the	http://r thelp.co	nvidia.cus om/app/a /detail/a_ 7	D	I-GPU 16/94
CV Scoring 0-1 Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring 0-1 Scale	1-2	2- 3	3	3-4 4-5 5-6		6-7	7-8	8-9	9-10	
	08/11/20		7.2	GeF NVI GPU R34 and 375 vuln kern (nvl han Dxg 0x1 valu is us vali inde arra den pote of p Ref 201 For Qua GeF NVI GPU R34 and 375 vuln Valu is us vali inde arra den pote of p valu GeF NVI GPU GPU GPU GPU GPU GPU GPU GPU GPU GPU	dro, NVS, orce production of Display of Disp	lucts, lows Driver 342.00 Fore ins a in the layer laye	http://ithelp.conswers.id/4247	nvidia.cus om/app/a /detail/a_ 7	A-NV D 1811	I-GPU 16/96
Denial of Service	08/11/20	016	7.2	han Dxg 0x7 the buff validen pote of p Ref 201	ddmkm.s dler for DdiEscap 000170 v size of an er is not dated, lea ial of serv ential esca rivileges. erence: 0 6-8811 the NVID	e ID where input ding to vice or alation	http://r	nvidia.cus	A-NV	I-GPU

			(nvl) hand Dxgl 0x70 the s buffe valid deni pote of pr	kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x70001b2 where the size of an input buffer is not validated, leading to denial of service or potential escalation of privileges. Reference: CVE-2016-8809 For the NVIDIA					
Denial of Service	08/11/2016	7.2	For a Quade GeFo NVIII GPU R34 and 375. vuln kern (nvlo hand 0x70 valu an u is us valid inde arra deni pote of procession of pro		and lucts, lows Driver 342.00 fore ins a in the layer ys) e ID where a from e driver ut the aternal g to rice or alation	thelp.co	nvidia.cus om/app/a /detail/a_ /	D	I-GPU 16/97
Denial of Service; Overflow	08/11/2016	7.2	Quad GeFo NVII GPU R34 and	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a		thelp.co	nvidia.cus om/app/a /detail/a_ 7	D	I-GPU 16/98
CV Scoring 0-1 Scale	1-2 2-	3	3-4 4-5 5-6		6-7	7-8	8-9	9-10	

Denial of Service	08/11/2016	7.2	kernel mo (nvlddml- handler for DxgDdiEs 0x100000 value is p an user to is used w validation size input memcpy(stack buff overflow, denial of potential of priviles Reference 2016-88	sm.sys) or scape ID e9 where a assed from the driver ithout as the to) causing a fer leading to service or escalation ges. ee: CVE- 07		nvidia.cus		I-GPU
			R340 before and R375 and R375.63 continuous vulnerabilitation (nvlddmlandler for DxgDdiEs 0x50000) pointer proposed an user to is used wordidation	oroducts, Vindows lay Driver ore 342.00 before ontains a lity in the ode layer sm.sys) or scape ID 27 where a assed from o the driver ithout n, leading of service ial n of s.	_	om/app/a /detail/a_ 7	D 1811	16/99
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products,				D	I-GPU 16/100
CV Scoring 0-1 Scale	1-2 2-3	3	3-4 4-5		6-7	7-8	8-9	9-10

			GPU R34 and 375 vuln kern (nvl han Dxg 0x7 valu an u is us vali inde arra den pote of p Ref 201	DIA Wind Display 0 before R375 before .63 containerability nel mode ddmkm.s dler for DdiEscap 000014 vole passed is er to the sed without a containerability leading ial of servential escrivileges. erence: 0.6-8805	Driver 342.00 fore ins a in the layer tys) e ID where a from e driver out the iternal g to vice or alation	id/4247			
Denial of Service	08/11/20	16 7.	Qua GeF NVI GPU R34 and 375 vuln kerr (nvl han Dxg 0x1 mis bou allo to k lead serv esca priv Ref	the NVID dro, NVS, orce produce produc	and ducts, lows Driver 342.00 fore ins a in the layer sys) The ID where a variety can to write mory, nial of tential	thelp.co	nvidia.cus om/app/a /detail/a_ /	D	I-GPU 16/101
CV Scoring 0-1 Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service	08/11/2016	7.2	For the NVID Quadro, NVS, GeForce prod NVIDIA Wind GPU Display R340 before and R375 bef 375.63 contavulnerability kernel mode (nvlddmkm.shandler for DxgDdiEscap 0x7000194 value passed user to the drused without validation as index to an irrary, leading denial of serve potential escap of privileges. Reference: C 2016-7390	and ducts, lows Driver 342.00 fore ins a in the layer sys) e ID where a from a river is the iternal g to vice or alation	thelp.co nswers, id/4247		D 1811	I-GPU 16/102
Gain Privileges	08/11/2016	7.2	For the NVID Quadro, NVS, GeForce, and products, NV GPU Display on Linux R30 before 304.1 R340 before R361_93 before R361_93 before 370.2 contains a vulnerability kernel mode (nvidia.ko) h for mmap() vimproper inpudlidation mallow users to arb	Tesla IDIA Driver 14 32, 340.98, 367.55, ore 10d R370 8 in the layer andler where out ay o gain	thelp.co	nvidia.cus om/app/a /detail/a_ 6	D	I-GPU 16/103
CV Scoring 0-1 Scale	1-2 2-	3	3-4 4-5 5-6		6-7	7-8	8-9	9-10

				physical memory, leading to an escalation of privileges.						
					erence: (6-7290	CVE-				
Denial of Service	08/11/20	16	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential escalation of privileges. Reference: CVE- 2016-7388			thelp.co	nvidia.cus om/app/a /detail/a_ 7	D	7I-GPU .16/104
Denial of Service	08/11/20	16	7.2	For to Quade GeFo NVIII GPU R34d and 375. vuln kern (nvlohand Dxgl 0x60 valu user used	Reference: CVE- 2016-7388 For the NVIDIA Quadro, NVS, and GeForce products,		thelp.co	nvidia.cus om/app/a /detail/a_ 7	D	7I-GPU .16/105
CV Scoring 0-1 Scale	1-2	2-3		3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service	08/11/2016	6.1	Qua GeF imp sant para NVA caus serv (blu with Win driv Ref	the NVID dro, NVS, orce procestization of ameters in API supposes a denimite vice vulned escreen on the NV adows gravers.	and lucts, of the rt layer al of rability crash) VIDIA phics	thelp.co	nvidia.cus om/app/a /detail/a_ }	D	I-GPU 16/106
Denial of Service	08/11/2016	7.8	For Qua GeF ther Des serv exp vuli will ker dere a bl	the NVID dro, NVS, orce proces a Renktop denivice. A such loit of a nerable syresult in hel null poeference, bue screen erence: C.6-4959	and lucts, note al of cessful estem a ointer causing crash.	thelp.co	nvidia.cus om/app/a /detail/a_ }	D	I-GPU 16/107
Objective Develop	ment								
Little Snitch									
Little Snitch is a ho	• •								ications,
preventing or perm Overflow	15/11/2016	7.2					'speakerd	A-OB	I-
			Little Snitch version 3.0 through 3.6.1 suffer from a buffer overflow vulnerability that could be locally exploited which could lead to an escalation of privileges (EoP) and unauthorised ring0 access to the			eck.com wardle, 2016-i- problen	/patrick /defcon- got-99-	LITT	-
CV Scoring 0-1 Scale	1-2	2-3	3-4 4-5 5-6				7-8	8-9	9-10

CV Scoring 0-1 Scale	1-2 2-	-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10
Execute Code	04/11/2016	6.8	Pillow before 3.3.2 allows context-dependent attackers to execute arbitrary code by using the "crafted image file" approach, related to an "Insecure Sign Extension" issue affecting the ImagingNew in Storage.c	https://github.co m/python- pillow/Pillow/pu ll/2146/commits /5d8a0be45aad7 8c5a22c8d09911 8ee26ef8144af	PILLO 181116/110
Python Pillow: NA					
Heat is the main pr	ultiple composit		In OpenStack Heat, by launching a new Heat stack with a local URL an authenticated user may conduct network discovery revealing internal network configuration. Affected versions are <=5.0.3, >=6.0.0 <=6.1.0, and ==7.0.0. Reference: CVE-2016-9185		
Openstack Heat					
			"copyin" kernel API calls. Reference: CVE- 2016-8661		
			operating system. The buffer overflow is related to insufficient checking of parameters to the "OSMalloc" and		

			component. Reference: CVE- 2016-9190		
Overflow; Gain Information	04/11/2016	4.3	Pillow before 3.3.2 allows context-dependent attackers to obtain sensitive information by using the "crafted image file" approach, related to an "Integer Overflow" issue affecting the Image.core.map_bu ffer in map.c component. Reference: CVE-2016-9189	http://pillow.rea dthedocs.io/en/3 .4.x/releasenotes /3.3.2.html	A-PYT- PILLO 181116/111
Qemu	tualization whe	n execut	ing under the Xen h	ypervisor or using t	the KVM kernel
Denial of Service	04/11/2016	1.9	The rtl8139_cplus_trans mit function in hw/net/rtl8139.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) by leveraging failure to limit the ring descriptor count. Reference: CVE-2016-8910		A-QEM- QEMU 181116/112
Denial of Service	04/11/2016	1.9	The intel_hda_xfer function in hw/audio/intel- hda.c in QEMU (aka	NA	A-QEM- QEMU 181116/113
CV Scoring 0-1 Scale	1-2 2-	3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			allo OS to o ser loo cor an sar but poi Re	ick Emula ows local administ cause a de vice (infing p and CPU sumption entry wit ne value f ffer length inter posi ference: 16-8909	guest rators enial of nite U n) via h the or n and tion.				
Denial of Service	04/11/2016	1.9	me hw QE Em loc addresser Zer QE crainv div tha	tial_updat ters funct /char/set MU (aka (ulator) al al guest (ministrato ise a deni vice (divi o error an MU proce sh) via ve olving a ve ider grea in baud ba	ction in rial.c in Quick ellows of al of de-by-estors value of ter ase.	rg/?p=c =comm fe0c919	git.qemu.o qemu.git;a it;h=3592 Ocf27a81d 1f269553	QEMI	
Denial of Service	04/11/2016	1.9	The root fund hww ker Qualle OS to e ser boot QE craalev	The rocker_io_writel function in hw/net/rocker/roc ker.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of- bounds read and QEMU process crash) by leveraging failure to limit DMA buffer		NA		A-QE QEMI 1811	
CV Scoring O-1 Scale	1-2 2-	-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			oigo.		
			size. Reference: CVE-		
Denial of Service	04/11/2016	1.9	The rc4030_write function in hw/dma/rc4030.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-byzero error and QEMU process crash) via a large interval timer reload value. Reference: CVE-2016-8667	NA	A-QEM- QEMU 181116/116
Denial of Service	04/11/2016	1.9	The v9fs_iov_vunmarsh al function in fsdev/9p-iov-marshal.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) by sending an empty string parameter to a 9P operation. Reference: CVE-2016-8578	NA	A-QEM- QEMU 181116/117
Denial of Service	04/11/2016	1.9	Memory leak in the v9fs_read function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS	http://git.qemu.o rg/?p=qemu.git;a =commit;h=e95c 9a493a5a8d6f96 9e86c9f19f80ffe 6587e19	A-QEM- QEMU 181116/118

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

				ministrato use a deni					
				vice (mer					
				nsumption	-				
				ctors relat	-				
				I/O read					
				eration.					
				ference:	CVE-				
			20	16-8577					
Denial of Service	04/11/2016	1.9	fur hw in Qu all OS to ser loc	e xhci_rin nction in n/usb/hcc QEMU (ak ick Emula ows local administ cause a de vice (infin op and QE ocess cras	d-xhci.c ta ator) guest rators enial of nite MU	rg/?p=0 =comm 3d44e4	git.qemu.o qemu.git;a it;h=05f4 bc26611c 1726e483 ce	QEM 1811	
			lev to of Re (T:	veraging falimit the ralimit the ralimit the range quest Blook (RB) to proference: 16-8576	ailure number sfer cks ocess. CVE-				
Sparkjava									
Spark			6			,	, ,		
Spark is a micro we									
Directory Traversal	04/11/2016	5	vu Sp rea via the Re	rectory trailnerability ark 2.5 all mote attace at arbitra a (dot ce URI. eference: 16-9177	y in lows ckers to ry files lot) in	m/perv	/github.co vendel/sp ues/700	SPAR	
Sybase									
Adaptive Server En SAP ASE (Adaptive S known as Sybase DI by Sybase Corporati	Server Enterpri B or ASE, is a re	lational	mod	el databas					
SQL Injection	03/11/2016	7.5	_	P ASE 16.	0 SP02	https://	/www.tru	A-SY	В-
CV Scoring 0-1 Scale	1-2 2	-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Torodata			versions allow attackers who own SourceDB and		ources/ Advisor ories/T	com/Res 'Security- ries/Advis WSL2016 id=8409		PT 16/121
Teradata								
Studio Express Teradata Studio Ex Teradata, and Hado desktop. It is built o	op Database sy	stems a	nd allows the	data to				
NA	10/11/2016	7.2	The installar script studioexpre I for Teradar Studio Expr 15.12.00.00 files in /tmp insecurely. A malicious lo could create symlink in / and possibly clobber syst or perhaps of privileges. Reference: 2016-7490	ssinstal ta ess creates A cal user a tmp dem files elevate CVE-		www.vapi om/advis ?v=174	STUD	
Virtual Machine A virtual machine is and applications. The	ne virtual mach	ine is co	mprised of a	e e e e e e e e e e e e e e e e e e e	_	_	_	_
and is backed by the Execute Code	10/11/2016	10	Teradata Vin Machine Community v15.10's per /opt/terada	Edition l script ta/gsct		www.vapi om/advis ?v=173	VIRT	
CV Scoring 0-1 Scale	1-2 2	-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Execute Code	10/11/20	016	7.2	manner, lead to el code exec Reference 2016-74 Teradata Machine Commun v15.10 ha insecure permissio /etc/lum mgr. The allow a lo modify it and exect	in insecure this may evated cution. ce: CVE- 89 Virtual ity Edition as file ons on inex/pkg se could ocal user to s contents ute ds as root. ce: CVE-	_ , ,	www.vapi om/advis ?v=172	VIRT	
		(Opera	ting Syst	em (OS)				
Canonical; Debian	; Linux; R	edhat							
Ubuntu Core; Ubun Aus; Enterprise Lin Ubuntu is a Debian source Linux open workstations and m	ux Eus; En based Linu ating syst	<i>terpri</i> ix Ope em fo	i se Lin t rating or use	ux Long Lij System; Er	f e; Enterpri iterprise Li	se Linux nux is an <u>y</u>	Tus y distribut	ion of t	he open
Gain Privileges	10/11/20		7.2	4.8.3 allo users to a privilege leveragin incorrect of a copy (COW) fe	c in the rnel 2.x 4.x before ws local gain s by g handling on-write ature to a read-only mapping, ted in the ctober	m/torva /comma	github.co alds/linux it/19be0e 7d8eb678 bc7d67ed	UBUN 1811	
				COW."					

				ference: (16-5195	CVE-				
Cisco			20	10-3173					
	» N Δ								
Asr 5000 Software Denial of Service	2: NA 03/11/20	016 5	the Sta ASI rou Pro (DI an una rem cau the ses dis res par ser cor vull affe 550 Data Car rur 18. Infe CSO Kne Rel 19. 20. Kne Rel 18. 18. 19. 19. 20. 20. 20.	ulnerability Slowpath rOS for Cit R 5500 Setters with ocessing Co CC2) could authenticate a subscribe sions to be connected ulting in a citial denial vice (DoS adition. The rability ects Cisco Co devices a Process rd 2 (DPC) aning Star Cormations Cvb12081 own Affect eases: 18 5.0 20.0.2 2.3 21.0.0 own Fixed eases: 18 7.4.65030 8.M0.650 5.M0.650 5.M0.650 2.3 20.2.3	n of isco cries Data Card 2 d allow ated, cker to et of er be d, a ll of) his 7 ASR swith sing 2) cos . More cted .7.4 2.64048 b. d7.4 b. 65092 23 50 8.64982 7	o.com/s enter/c		-	-ASR 5- 16/126
				2.a4.653(
CV Scoring 0-1 Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			20.3.M0.64984		
			20.3.M0.65029		
			20.3.M0.65037		
			20.3.M0.65071		
			20.3.T0.64985		
			20.3.T0.65031		
			20.3.T0.65043		
			20.3.T0.65067		
			21.0.0 21.0.0.65256		
			21.0.M0.64922		
			21.0.M0.64983		
			21.0.M0.65140		
			21.0.V0.65150		
			21.1.A0.64932		
			21.1.A0.64987		
			21.1.A0.65145		
			21.1.PP0.65270		
			21.1.R0.65130		
			21.1.R0.65135		
			21.1.R0.65154		
			21.1.VC0.65203		
			21.2.A0.65147.		
			Reference: CVE-		
			2016-6455		
Ios Xe IOS XE represents to used on most Cisco			n of Cisco's pre-emine work switches.	ent IOS operating sy	stem which is
Execute Code;	03/11/2016	10	Vulnerability in the	https://tools.cisc	O-CIS-IOS X
Overflow			Transaction	o.com/security/c	181116/127
			Language 1 (TL1)	enter/content/Ci	
			code of Cisco ASR	scoSecurityAdvis	
			900 Series routers	ory/cisco-sa-	
			could allow an	20161102-tl1	
			unauthenticated,		
			remote attacker to		
			cause a reload of,		
			or remotely		
			execute code on,		
			the affected system.		
			This vulnerability		
			affects Cisco ASR		
			900 Series		
			Aggregation		
			Services Routers		
		the second second	Services Routers		
			(ASR902, ASR903, and ASR907) that		

4-5

3-4

6-7

7-8

8-9

9-10

5-6

2-3

1-2

CV Scoring Scale

0-1

Microsoft

Windows 10; Windows 7; Windows 8.1; Windows Rt 8.1; Windows Server 2008; Windows Server 2012; Windows Server 2016; Windows Vista

Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems, each of which cater to a certain sector of the computing industry with the OS typically associated with IBM PC compatible architecture.

Gain Informa	tion	10/11/20	016	2.1		Vir	tual Secui	re	http://t	echnet.m	O-MI	G-
									icrosoft	.com/en-	WIND	00
						Wi	ndows 10	allows	us/secu	rity/bull	1811	16/128
						loc	al users to)	etin/ms	16-137		,
						obt	ain sensit	tive	,			
						inf	ormation	via a				
						cra	fted appli	cation.				
							a "Virtual					
						Mo	de Inforn	nation				
							closure	10.01011				
							lnerability	7."				
							ference: (
							16-7220					
Gain Privileg	es	10/11/20	016	7.2		Th	e kernel-r	node	http://t	echnet.m	O-MI	Ĵ-
						dri	vers in Mi	icrosoft	icrosoft	.com/en-	WIND	00
						Windows Server		us/security/bull		1811	16/129	
						2008 R2 SP1,		etin/ms	16-135		,	
CV Scoring	0-1	1-2	2-3	2	2	-4	4-5	5-6	6-7	7-8	8-9	9 -1 0
Scale	0-1	1-2	2-0	,	- 3	-1	4-3	3-0	0-7	7-0	6-9	9-10

				Windows 10 1511, and 10					
Gain Information	10/11/20	16	1.9	Bowser.sys is kernel-mode drivers in M Windows Vi Windows Se 2008 SP2 an SP1, Window SP1, Window Windows Se 2012 Gold a Windows R	e icrosoft sta SP2, erver nd R2 ws 7 ws 8.1, erver nd R2, I 8.1,	icrosoft us/secu	technet.m c.com/en- urity/bull s16-135	0-MI WINI 1811	
Gain Privileges	10/11/20	016	7.2	Security Aut Subsystem Sub	Service rvice v." CVE- od) in lindows lindows SP2 SP1, 1, erver nd R2, F 8.1, D Gold, 607, vs DLL ich users leges ied ME	icrosoft us/secu	technet.m c.com/en- nrity/bull s16-130	0-MI WINI 1811	

				and Window Server 2016 local users to obtain sensi- information crafted appliaka "Window Bowser.sys Information Disclosure Vulnerability Reference: 2016-7218	allows o tive via a ication, ws				
Gain Privileges	10/11/201	6 7.	2	The kernel-r drivers in M Windows Vi- Windows Se 2008 SP2 an SP1, Window SP1, Windows Se 2012 Gold an Windows RI Windows 10 1511, and 10 and Window Server 2016 local users to privileges vi crafted appliaka "Win32A Elevation of Privilege Vulnerability Reference: 2016-7215	icrosoft sta SP2, rver d R2 vs 7 vs 8.1, rver nd R2, 607, s allow o gain a a ication, s	icrosoft us/secu	technet.m .com/en- arity/bull s16-135	O-MI WINI 1811	
Bypass; Gain Information	10/11/201	6 2.	1	The kernel-r drivers in M Windows Vi Windows Se 2008 SP2 an SP1, Window SP1, Window Windows Se 2012 Gold an	icrosoft sta SP2, rver d R2 vs 7 vs 8.1, rver nd R2,	icrosoft us/secu	technet.m .com/en- rity/bull s16-135	O-MI WINI 1811	
CV Scoring 0-1 Scale	1-2	2-3	3-4	4 4-5	5-6	6-7	7-8	8-9	9-10

			1 a S lo b p m c: a I li D V R 2	Vindows 10 511, and 10 nd Window erver 2016 ocal users to ypass the A rotection nechanism rafted applia ka "Win32l nformation isclosure ulnerability eference: 016-7214	607, 78 allow o SLR via a ication, c V." CVE-				
Execute Code	10/11/2016	9.3	VVS aa VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV	licrosoft Wista SP2, Werver 2008 and R2 SP1, Vindows 7.5 Vindows Sevendows R7 Vindows R7	SP1, 1, rver nd R2, 881, 9 Gold, 607, 78 allow ckers to trary rafted ka emote ion y."	icrosoft us/secu	technet.m .com/en- arity/bull s16-130	O-MI WINI 1811	
Gain Information	10/11/2016	4.3	M V S a V V	tmfd.dll in licrosoft W ista SP2, W erver 2008 nd R2 SP1, Vindows 7 S Vindows Se Vindows Se 012 Gold a	indows SP2 SP1, 1, rver	icrosoft us/secu	echnet.m .com/en- rity/bull s16-132	0-MI WINI 1811	
CV Scoring 0-1 Scale	1-2 2	-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring 0-1 Scale	1-2	2-3		3-4	4-5	5-6	6-7	7-8	8-9	9-10
Overflow; Gain Privileges	10/11/20		9.3	and Ser rer obtainfa provide the provide t	11, and 10 d Window ver 2016 note attactain sensition ocess mere a crafted pe font or e, aka "Oppe Font ormation oclosure linerability ference: 16-7210 e Commo e System ver in Michael SP2 and 1, Windows Sendows SP2 and 1, Windows Sendows RT and 10 d Windows RT and 10 d Windows Sendows RT and 10 d Windows RT and	allows ckers to tive from nory Open a web en y." CVE- n Log (CLFS) crosoft sta SP2, croso	icrosoft us/secu etin/ms	technet.m com/en- crity/bull s16-134		00
				Wi	ndows R7 ndows 10	Gold,				

			CV CV CV CV and 33- Re 20	ference: 16-7184	334, 335, 338, 340, 342, 16-				
Overflow; Gain Privileges	10/11/20	016 9.3	File dri Wi Wi 200 SP1 SP2 Wi 20 Wi Wi 15 and Ser loc pri cra aka Con Sys Ele Pri Vui diff vul CV	e Commo e System ver in Mic ndows Vi ndows Se 08 SP2 an 1, Window 1, Windows Se 12 Gold a ndows 10 11, and 10 11 window ver 2016 al users to vileges vi fted appl a "Window vation of vilege lnerability ferent nerability ferent nerability E-2016-3 E-2016-3 E-2016-3 E-2016-3 E-2016-3 E-2016-3 C-2016-3 E-2016-3	(CLFS) crosoft sta SP2, erver ad R2 ws 7 ws 8.1, erver ad R2, F 8.1, O Gold, 607, ws a allows o gain a a ication, ws g File er y," a y than 026, 332, 333, 334, 335, 338, 340, 342,	icrosoft us/secu	technet.m c.com/en- urity/bull s16-134	O-MIC WIND 1811	
CV Scoring 0-1 Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE- 2016-3343		
Overflow; Gain Privileges	10/11/2016	9.3	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3333, CVE-2016-3334, CVE-2016-3334, CVE-2016-3343, and CVE-2016-3343, and CVE-2016-7184. Reference: CVE- 2016-3342	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-134	O-MIC- WINDO 181116/141
Overflow; Gain Privileges	10/11/2016	9.3	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-134	0-MIC- WINDO 181116/142
CV Scoring 0-1 Scale	1-2 2-	3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

Overflow; Gain	10/11/20	016	9.3	SP W 20 W 15 an Se loo pr cra ak Co Sy Elo Pr Vu diff vu CV CV CV CV CV CV CV CV CV CV CV CV CV	1, Window 1, Window 1, Window 1, Window 12 Gold a 11, and 10 12, and 10 13, and 10 14, and 10 15, and 10 16, and 10 17, and 10 18, a	ws 8.1, erver and R2, F 8.1, Gold, 607, ws allows o gain a a ication, ws g File er y," a y than 026, 332, 333, 334, 335, 338, 342, 343, 16- CVE-	http://t	technet.m	O-MI	C-
				71	84.					
						CVE-				
Overflow; Gain Privileges	10/11/20	016	9.3	Th Fil dr W 20 SP SP W 20 W W		(CLFS) crosoft sta SP2, erver ad R2 ws 7 ws 8.1, erver and R2, F 8.1, O Gold,	icrosoft us/secu	technet.m c.com/en- arity/bull s16-134	WINI	
CV Scoring 0-1 Scale	1-2	2- 3	3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Overflow; Gain Privileges	10/11/20	016 9.:	loce pri cra aka Coi Sys Ele Pri Vu diff vul diff vul CV CV CV CV CV CV CV CV CV Sys and 71% Re 20 SP	ver 2016 al users to vileges vi fted applia "Window vation of vilege inerability E-2016-3 E-2	o gain a a ication, ws g File er y," a y than 026, 332, 333, 334, 335, 340, 342, 343, 16- CVE- In Log (CLFS) crosoft sta SP2, rver ld R2 vs 7 vs 8.1, rver ld R2, rver ld R3, rver ld R4, rver ld R5, rver ld R6, rver ld R6, rver ld R6, rver ld R6, rver ld R7, rver ld R6, rver ld R7, rver ld R9,	icrosoft us/secu	technet.m t.com/en- arity/bull s16-134	WIND	
CV Scoring 0-1 Scale	1_7	7_3	3_4	/1_5	5.6	67	7 0	0.0	

			Vuldiffi vul CV: CV: CV: CV: CV: CV: CV: Re	vilege Inerability Ferent nerability E-2016-3 E-2016-3 E-2016-3 E-2016-3 E-2016-3 E-2016-3 E-2016-3 F-2016-3 F-2016-3 F-2016-3	than 026, 332, 333, 334, 338, 340, 342, 343,				
Overflow; Gain Privileges	10/11/20	9.	The File dri Wi Wi 200 SP2 SP2 Wi 200 Wi Wi 155 and Ser loc pri cra aka Con Sys Ele Pri Vul diff vul CV2 CV2	e Common e System (ver in Mice andows Vision ows Se 108 SP2 and 1, Windows 12 Gold andows R7 andows R7 andows 10 11, and 16 d Windows ver 2016 al users to vileges vision fted applia "Windows the Drive vation of vilege (nerability) ferent nerability Ferent nerability E-2016-3 E-2016-3	(CLFS) crosoft sta SP2, rver d R2 vs 7 vs 8.1, rver nd R2, 607, rs allows o gain a a ication, vs g File er y," a r than 026, 332, 333,	icrosoft us/secu	cechnet.m .com/en- arity/bull s16-134	O-MI WINI 1811	
CV Scoring 0-1 Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Scale	CVE-2016-3343, and CVE-2016-7184. Reference: CVE-2016-3334	CVE-2016-3338, CVE-2016-3340, CVE-2016-3342,
---	--	--

Overflow; Gain Privileges	10/11/2016	9.3	The Common File System I driver in Mid Windows Vis Windows Se 2008 SP2 and SP1, Windows SP1, Windows SP1, Windows R1 Windows R1 Windows R1 Windows R1 Windows Server 2016 local users to privileges vicrafted appliaka "Windows Common Log System Drive Elevation of Privilege Vulnerability different vulnerability different vulnerability CVE-2016-3 CVE-2016	(CLFS) crosoft sta SP2, rver ld R2 vs 7 vs 8.1, rver ld R2, F 8.1, Gold, 607, vs allows o gain a a ication, vs g File er vy," a v than 026, 333, 334, 335, 338, 340, 342, 343, 16-	icrosoft	rechnet.m .com/en- arity/bull s16-134	O-MINI 1811	
Overflow; Gain Privileges	10/11/2016	9.3	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1,		http://technet.m icrosoft.com/en- us/security/bull etin/ms16-134		O-MIC- WINDO 181116/148	
CV Scoring 0-1 Scale	1-2 2-	3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

					202 Win Win 152 and Ser loca prir cra aka Con Sys Ele Prir Vul diffi vul CVI CVI CVI CVI CVI CVI CVI CVI CVI CVI	ference:	nd R2, 78.1, 600d, 607, 78 allows o gain a a ication, vs g File er y," a 7 than 332, 333, 334, 335, 334, 340, 342, 343, 16-				
Execute Code	10/11/20	016	9.3		2016-0026 Microsoft Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Video Control Remote Code Execution		icrosoft us/secu	technet.m t.com/en- trity/bull s16-131	WINI		
CV Scoring 0-1 Scale	1-2	2-3	3	3-	-4	4-5	5-6	6-7	7-8	8-9	9-10

			Re	lnerability ference: 16-7248	CVE-				
Bypass	10/11/2016	10/11/2016 5			indows vs Gold dows dows 1, and erver bypass oot via a policy, Boot	http://technet.m icrosoft.com/en- us/security/bull etin/ms16-140		O-MIC- WINDO 181116/150	
Gain Privileges	10/11/2016	5 3.6	Dr Wi Wi 20 Wi Wi 15 an Sei no res file loc pri cra aka Ele Pri Vu	Reference: CVE- 2016-7247 Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka "VHD Driver Elevation of Privilege Vulnerability." Reference: CVE-		icrosoft us/secu	technet.m .com/en- arity/bull s16-138	O-MI WINI 1811	
CV Scoring 0-1 Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Gain Privileges	10/11/20	016	3.6	r e c v "" M C V	remote attace execute arbitected via a croweb site, akade Media Found Memory Corruption Vulnerability Reference: Q016-7217	ckers to trary afted a dation y." CVE-	kers to rary afted dation		C-	
Execute Code; Overflow; Memory Corruption	Overflow; Memory		9.3	ii V V 2 V V 1 a	Media Found in Microsoft Windows Se Windows RT Windows RT Windows 10 1511, and 16 and Window Server 2016	l, rver nd R2, 18.1, Gold, 607,	icrosoft	.com/en- rity/bull	WINI	
Gain Privileges	10/11/20		3.6	II VV VV 11 aa S rr rf fl II F C C aa H F V V	Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka "VHD Driver Elevation of Privilege Vulnerability." Reference: CVE- 2016-7223 Media Foundation in Microsoft http://technet.m icrosoft.com/en-		1811	WINDO 181116/152		

Gain Privileges	10/11/203	16	7.2	Re 20 Ta Mi 10 16 Se loo pr cry pa ak Sc Ell Pr Vu Re	Privilege Vulnerability." Reference: CVE- 2016-7225 Task Scheduler in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to gain privileges via a crafted UNC pathname in a task, aka "Task Scheduler Elevation of Privilege Vulnerability." Reference: CVE- 2016-7222		icrosoft us/secu	technet.m .com/en- irity/bull s16-130	O-MI WINI 1811	
Gain Privileges	10/11/202	16	3.6	no re fill look process as the proce	_	ess to allows o gain a a ication, river Y." CVE- I Disk indows I 1, and Indows o does Vess to allows o gain a a ication, river	icrosoft us/secu	cechnet.m .com/en- nrity/bull s16-138	O-MI WINI 1811	

Gain Privileges	10/11/2016	2.1	The kernel API in	http://technet.m	O-MIC-
			Microsoft Windows	icrosoft.com/en-	WINDO
			Vista SP2, Windows	us/security/bull	181116/157
			Server 2008 SP2	etin/ms16-139	
			and R2 SP1, and		
			Windows 7 SP1		
			mishandles		
			permissions, which		
			allows local users		
			to gain privileges		
			via a crafted		
			application, aka		
			"Windows Kernel		
			Elevation of		
			Privilege		
			Vulnerability."		
			Reference: CVE-		
			2016-7216		

Samsung

Samsung Mobile

Samsung is the largest mobile phone maker in its home market of South Korea, and the third largest in the world. In addition to mobile phones and related devices, the company also manufacturers things such as televisions, cameras, and electronic components.

NA	03/11/2016	7.8	A vulnerability on	http://security.s	O-SAM-
			Samsung Mobile	amsungmobile.co	SAMSU
			L(5.0/5.1) and	m/smrupdate.ht	181116/158
			M(6.0) devices with	ml#SMR-SEP-	
			the Exynos7420	2016	
			chipset exists		
			because of a NULL		
			pointer		
			dereference in the		
			fimg2d driver. The		
			patch (aka "SVE-		
			2016-6248:		
			SystemUI Security		
			issue") verifies if		
			the object is null		
			before		
			dereferencing it.		
			Reference: CVE-		
			2016-7160		
Denial of Service;	11/11/2016	7.8	Integer overflow in	http://security.s	O-SAM-
Overflow			SystemUI in	amsungmobile.co	SAMSU
			KK(4.4) and	m/smrupdate.ht	181116/159

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

	L(5.0/5.1) on	ml#SMR-NOV-	
	Samsung Note	2016	
	devices allows		
	attackers to cause a		
	denial of service		
	(UI restart) via		
	vectors involving		
	APIs and an activity		
	that computes an		
	out-of-bounds		
	array index, aka		
	SVE-2016-6906.		
	Reference: CVE-		
	2016-9277		