Book	National C	ritical		on Infras EVE Repor		re Protec	ction Ce	ntre
CV Scoring Scale : 3-10 15 May -15 Jun 2018 Vulnerability Publish Date CVSSS Description & CV ID Refer								5 No.11
Vulnerability Type(s)	Publish Date	cvsss	Descri	ption & CV	ID	Referenc	e/Patch	NCIIPC ID
yr (c)			Appli	cation				
Dolibarr								
Dolibarr	20.05.0040	4.0			(Maa)	1	1	
XSS	22-05-2018	4.3	Cross-site vulnerability 7.0.2 allows inject arbitr HTML via parameter adherents/ca ID:CVE-2018	remote atta ary web s the for rtes/carte.p	ackers to script or userlogin to	https://sysm/news/la 05-21-cve- 10095-doli injection- vulnerabili https://git Dolibarr/d ommit/1dc 687cfe647 720419823 https://git Dolibarr/d lob/7.0.2/0 g	ab/2018- 2018- ibarr-xss- ty/ hub.com/ olibarr/c c466e1fb de4af891 3ed56 hub.com/ olibarr/b	A-Dol- Dolib/18- 06-18/1
Foxitsoftware						5		
Foxit Reader								
Execute Code Gain Information	17-05-2018	4.3	This vulnera attackers to information installations 9.0.0.29935. required to vulnerability must visit a open a maliciflaw exists w U3D files. The lack of puser-supplied result in a reallocated dattacker can conjunction	disclose on vo of Foxit User inter- to exploi in that the malicious ous file. The rithin the p e issue resion oper valid d data whe ata struct	sensitive ulnerable Reader action is it this ne target page or e specific arsing of ults from dation of nich can end of an ure. An	https://zer ative.com/ s/ZDI-18-3 https://ww oftware.com rt/security bulletins.pl	advisorie 881 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/2
CV Scoring Scale (C	VSS)	3-	4 4-5	5-6	6-7	7-8	8-9	9-10
	(s): CSRF-Cross Site	Request For	rgery; Dir. TravDi	rectory Trave	rsal; DoS-Der	nial of Service;	NA- Not Appli	cable; Sql-SQL

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	cvsss		Descrip	otion & CV	ID	Reference	e/Patch	NCIIPC ID
			the prod	context cess. Wa		context AN-5494.			
Foxit Reader, P	hantom Pdf								
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the addLink method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5379. CVE-ID:CVE-2018-9944				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security- bulletins.ph	advisorie 28 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/3
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 18 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/4
CV Scoring Scale (C	VSS)	3	4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descri	otion & CV	ID	Reference	e/Patch	NCIIPC ID
Execute Code	17-05-2018	6.8	attacod of Finter this targ or specific the per object under pro	ckers to e on vulneration is vulneral open a recific flaw field me existence forming open. An attribute the concess. With the concess.		arbitrary tallations 935. User to exploit that the ious page file. The issue validating the prior to on the leverage cute code e current AN-5382.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 29 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/5
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of CPDF_Object objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5414.				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 35 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/6
Execute Code	17-05-2018	6.8	Th atta cod of F inte	nis vulnera nckers to ne on vuln Foxit Read eraction is	bility allow execute erable inser 9.0.0.299 required to bility in	rs remote arbitrary tallations 935. User to exploit	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security-	advisorie 23 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/7
CV Scoring Scale (CV	/SS)	3	4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
Execute Code	17-05-2018	6.8	or spe har The pro sup a t atta vuli und pro CVI Th atta	open a recific flaw adling of e issue resiper valid policed data experiments of the concrability der the concrability experiments. We E-ID:CVE-2 ais vulneral exckers to	which can usion cond no leveral to execute the state of t	file. The thin the lements. The lack of fuser-result in ition. An age this ate code e current AN-5373.	https://zer ative.com/a s/ZDI-18-3	odayiniti advisorie	A-Fox- Foxit/18- 06-18/8
			code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the absPageSpan method. The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5372. CVE-ID:CVE-2018-				https://ww oftware.cor rt/security- bulletins.ph	w.foxits n/suppo	
Execute Code	17-05-2018	6.8	cod of F inte this targ or spe	nis vulnera ackers to le on vuln Foxit Read eraction is s vulnera get must v open a	bility allow execute nerable ins er 9.0.0.299 required this in isit a malicimalicious exists wif the a	arbitrary tallations 935. User to exploit that the fous page file. The	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 15 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/9
CV Scoring Scale (C	CV Scoring Scale (CVSS)			4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			the exist per obj this und pro	lack of stence of forming of ect. An at s vulnerable der the corocess.	issue results of validate an object operations tacker can illity to execute the as ZDI-C. 2018-1177	ing the prior to on the leverage cute code e current AN-5488.			
Execute Code	17-05-2018	6.8	atta cod of I inte this targ or spe har me the exis per obj this unc pro	ackers to le on vulred le on vulred le caction is so vulnera get must vecific flaw adding of thod. The lack of forming ect. An at so vulnerable der the concess.	e issue result of validate an object operations tacker can illity to execute the context of the	arbitrary tallations 035. User to exploit that the tous page file. The thin the addField alts from ing the prior to on the leverage cute code e current AN-5489.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 16 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/10
Execute Code	17-05-2018	6.8	The attacod of I into this targ or special attached use res	nis vulnerance ckers to le on vulnerance con is vulnerance con a period for the control of per-supplied out in a	bility allow execute nerable insers of the layout the layout the layout data where we have the layout the layo	rs remote arbitrary tallations 935. User to exploit that the tous page file. The thin the ut sheet ults from dation of nich can confusion	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 24 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/11
CV Scoring Scale (C	VSS)	3		4-5	5-6	6-7	7-8	8-9	9-10

Execute Code 17	17-05-2018	6.8	leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5374. CVE-ID:CVE-2018-9940 This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page	https://zerodayiniti ative.com/advisorie s/ZDI-18-327 https://www.foxits oftware.com/suppo	A-Fox- Foxit/18- 06-18/12
Execute Code 17	17-05-2018	6.8	attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page	ative.com/advisorie s/ZDI-18-327 https://www.foxits	Foxit/18-
			or open a malicious file. The specific flaw exists within the handling of the openList method. The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5377. CVE-ID:CVE-2018-9943	rt/security- bulletins.php	
Execute Code 17	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the record append method. The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-	https://zerodayiniti ative.com/advisorie s/ZDI-18-325 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/13

Vulnerability Type(s)	Publish Date	CVSSS	Description	a & CV ID	Reference/Patch	NCIIPC ID
			CAN-5375. CVE 9941	-ID:CVE-2018-		
Execute Code	17-05-2018	6.8	This vulnerability attackers to execute code on vulnerability of Foxit Reader 9. Interaction is required this vulnerability target must visit a or open a malic specific flaw exity handling of the method. The issues the lack of proper user-supplied daresult in a typic condition. An leverage this very execute code under the current process.	cute arbitrary de installations 0.0.29935. User aired to exploit in that the malicious page tious file. The sts within the record remove the results from the realidation of the which can appear confusion attacker can alinerability to or the context of	https://zerodayinit ative.com/advisorie s/ZDI-18-326 https://www.foxits oftware.com/support/security- bulletins.php	Foxit/18- 06-18/14
Execute Code	17-05-2018	6.8	This vulnerability attackers to execute on vulnerability of Foxit Reader 9.0 interaction is required this vulnerability target must visit a or open a malic specific flaw existandling of borderColor at issue results from validating the exobject prior to operations on the attacker can vulnerability to under the context.	cute arbitrary de installations 0.0.29935. User uired to exploit in that the malicious page clous file. The sts within the the XFA ctribute. The mathematic he object. An aleverage this execute code of the current ZDI-CAN-5436.		Foxit/18- 06-18/15
CV Scoring Scale (C		3	4-5	5-6 6-7	7-8 8-9	9-10

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s) Publish Date	cvsss		Descrij	ption & CV	ID	Reference	e/Patch	NCIIPC ID
Execute Code 17-05-2018	6.8	atta cod of I inte this tar; or spe pai res val: wh the atta vul unc pro	ackers to le on vulneration is vulneral get must versing of eluts from idation of ich can researcher can acker can erability der the concess.	to execuntext of the	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.ph	A-Fox- Foxit/18- 06-18/16		
Execute Code 17-05-2018	6.8	The attacood of I into this tary or special issue processing a tatta vuluno processing processing and tattacontrol of the attacontrol of the attac	nis vulneral ackers to le on vulneral foxit Read eraction is secured by the confidence of the confiden	bility allow execute terable instered execute terable instered to execute the execute to execute the execute to execute the execute to execute the	rs remote arbitrary tallations 935. User to exploit that the lous page file. The thin the lack of f user-result in ition. An age this ite code e current AN-5370.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.ph	advisorie 20 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/17
Execute Code 17-05-2018	6.8	Thatta cod of l	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User				advisorie 00	A-Fox- Foxit/18- 06-18/18
CV Scoring Scale (CVSS)	3-4	interaction is required to exploit https://www.foxits -4 4-5 5-6 6-7 7-8 8-9						9-10

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID Res	eference/Patch NCIIPC ID
Execute Code	17-05-2018	6.8	target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG images embedded inside U3D files. The issue results from the lack of proper validation of usersupplied data which can result in a memory access past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5422. CVE-ID:CVE-2018-10490 This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page rt/set	vare.com/suppo security- letins.php Discrete dayiniti re.com/advisorie DI-18-375 Discrete dayiniti re.com/adviso
Execute Code	17-05-2018	6.8	attackers to execute arbitrary ative	os://zerodayiniti re.com/advisorie DI-18-405 A-Fox- Foxit/18- 06-18/20
			interaction is required to exploit http: this vulnerability in that the oftw target must visit a malicious page rt/se	os://www.foxits vare.com/suppo security- letins.php
CV Scoring Scale (C	VSS)	3	4 4-5 5-6 6-7	7-8 8-9 9-10

Vulnerability Type(s)	Publish Date	cvsss		Descrip	otion & CV	ID	Reference	e/Patch	NCIIPC ID
			par issu pro sup a t atta vuli und pro	rsing of Place results oper valid oplied data sype confunction can be confused by the confused	to execunter to the	ents. The lack of fuser-result in ition. An ge this ate code e current AN-5586.			
Execute Code	17-05-2018	6.8	The attacod of Finter this targ or specific properties attaced to the attaced properties attaced to the attaced	nis vulnerand ckers to be on vulneral consisted as a v	bility allow execute erable inser 9.0.0.299 required to execute the execut	rs remote arbitrary tallations 935. User to exploit that the tous page file. The thin the lements. The lack of fuser-result in the tion. An age this te code e current AN-5371.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 21 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/21
Execute Code	17-05-2018	6.8	The attacod of Finter this targ or specific part U31	nis vulnerand ckers to le on vulneral contion is vulneral get must vice open a recific flawersing of the lack of p	bility allow execute erable inser 9.0.0.299 required to bility in exist a malicious exists with exists	rs remote arbitrary tallations 935. User to exploit that the tous page file. The thin the Width in ults from dation of	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 80 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/22
CV Scoring Scale (CVSS) 3-4					5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			result in a write past the end of an allocated object. An attacked can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5483. CVE-ID:CVE-2018-9982		
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D Bone Weight Modifier structures. The issue results from the lack of proper validation of user-supplied data which can result in a write pass the end of an allocated structure An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5423 CVE-ID:CVE-2018-10491	ative.com/advisorie s/ZDI-18-401 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/23
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D Chain Index objects. The issue results from the lack of proper validation of user-supplied data which car result in a write past the end of an allocated object. An attacker can leverage this vulnerability to	ative.com/advisorie s/ZDI-18-387 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/24
		3-	4 4-5 5-6 6-7	7-8 8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descrij	otion & CV	ID	Reference	e/Patch	NCIIPC ID
			the CAl		under the c process. V CVE-ID:CV	Vas ZDI-			
Execute Code	17-05-2018	6.8	atta cod of I inte this targ or spe pai Me The pro sup a allo can exe the CAI	ackers to de on vuln Foxit Reade eraction is subset with the continue issue result option data write pasticated structure code ecute code en validation of the code ecute code en validation of the code ecute code en validation of the code ecute ecut	bility allow execute lerable inster 9.0.0.299 required to bility in isit a malicinalicious fexists will U3D CLO leads from the dation of which candidation to which candidations. And the condition of th	arbitrary tallations 935. User to exploit that the lous page file. The thin the D Base ructures. The lack of fuser-result in dof an attacker ability to context of Vas ZDI-	https://zer ative.com/a s/ZDI-18-33 https://ww oftware.com rt/security- bulletins.ph	advisorie 83 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/25
Execute Code	17-05-2018	6.8	atta cod of I inte this targ or spe pan Pro str from of res an atta	ackers to le on vuln Foxit Reade eraction is s vulneral get must vi open a r ecific flaw rsing o gressive uctures. m the lack user-suppl ult in a wi allocated		arbitrary tallations 935. User to exploit that the tous page file. The thin the Clod claration results validation which can ne end of ure. An ge this	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security- bulletins.ph	advisorie 99 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/26
CV Scoring Scale (CV	VSS)	3	4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descrij	otion & CV	ID	Reference	e/Patch	NCIIPC ID
			pro	cess. Wa	ntext of the as ZDI-C. 2018-1048	AN-5421.			
Execute Code	17-05-2018	6.8	atta cod of F inte this targ or spe par Pro issu pro sup a v allo leve exe the	ackers to le on vuln Foxit Readeraction is a vulneral get must victopen a recific flaw ring open a recific flaw ring open a results oper valicated object age this cute code a current N-5410.	bility allow execute erable inser 9.0.0.299 required to bility in isit a malicious exists with the enderthe exist and exist an	arbitrary tallations 935. User to exploit that the ious page file. The ithin the Clod ects. The lack of f user-result in d of an acker can bility to context of Vas ZDI-	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security- bulletins.ph	advisorie 93 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/27
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5431. CVE-ID:CVE-2018-9981				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security- bulletins.ph	advisorie 79 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/28
CV Scoring Scale (CVSS)		3-	4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSSS		Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID	
Execute Code	17-05-2018	6.8	cod of I into this tar; or spe pai The pric can exe the CAI	attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D Node objects. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5411. CVE-ID:CVE-2018-10484 This vulnerability allows remote https://zerodayiniti						
Execute Code	17-05-2018	6.8	The atta cool of I into this tary or specific properties a allowers the CAl	nis vulnera ackers to de on vuln Foxit Reade eraction is s vulneral get must vi open a n ecific flaw rsing of U3 e issue rest oper vali oplied data write pas ocated objected code	bility allow execute nerable inser 9.0.0.299 required to bility in isit a malicious exists with the candidation of which candidation of which candidation of the endect. An attast vulneral under the coprocess. Vice-ID:CV	arbitrary tallations 935. User to exploit that the tous page file. The thin the gobjects. The lack of fuser-result in dof an acker can bility to context of Vas ZDI-	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 84 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/30	
Execute Code	17-05-2018	6.8	Thatta cod of	nis vulnera ackers to le on vuln Foxit Read	bility allow execute nerable ins der 9.0.1.10 required t	arbitrary tallations 149. User	https://zer ative.com/a s/ZDI-18-3	advisorie 50	A-Fox- Foxit/18- 06-18/31	
CV Scoring Scale (C	VSS)	3		4-5	5-6	6-7				
or bearing beare (c	,									

Vulnerability Type(s)	Publish Date	cvsss		Descri	otion & CV	ID	Reference	e/Patch	NCIIPC ID
			targ or spe har Tex resu the per obje this und pro	get must vice open a recific flaw odding of (xtBox obults from texistence forming of ect. An attribute the context of the context of the context of the context.	bility in isit a malicimalicious malicious exists wice alculate a bjects. The lack of vof an object operations tacker can lity to execute to the as ZDI-C. 2018-9966	ious page file. The thin the ctions of the issue validating t prior to on the leverage cute code e current AN-5570.	oftware.cor rt/security- bulletins.ph		
Execute Code	17-05-2018	6.8	The attacood of I interest this targed har resist the perobjecthis under pro-	ackers to le on vulneral le on vulneral le caraction is vulneral get must vice open a le cific flaw adding of atBox object. An at sevulnerable der the concess.	bility allow execute lerable inster 9.0.1.10 required to bility in isit a malicious exists with the lack of vof an object operations tacker cantility to execute the lack of t	rs remote arbitrary tallations 149. User to exploit that the tous page file. The thin the ctions of the issue validating t prior to on the leverage cute code e current AN-5571.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	ndvisorie 51 w.foxits n/suppo	A-Fox- Foxit/18- 06-18/32
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Keystroke actions				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	ndvisorie 52 w.foxits n/suppo	A-Fox- Foxit/18- 06-18/33
CV Scoring Scale (CVSS)		3					7-8	8-9	9-10

Execute Code 17-05-2018		of TextBox objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5572.		
Execute Code 17-05-2018		CVE-ID:CVE-2018-9968		
	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of shift events. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5762. CVE-ID:CVE-2018-9975	https://zerodayiniti ative.com/advisorie s/ZDI-18-359 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/34
Execute Code 17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Text Annotations. When setting the point attribute the process does not properly validate the existence of an object prior to performing operations on the object. An attacker can	https://zerodayiniti ative.com/advisorie s/ZDI-18-342 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/35

leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5620. CVE-ID:CVE-2018-9958	Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the setAction method of Link objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5569. Execute Code 17-05-2018 6.8 This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Button elements. When parsing arguments passed to the resetDatamethod the process does not properly validate the existence of an object prior to performing operations on the				execute code under the context of the current process. Was ZDI- CAN-5620. CVE-ID:CVE-2018-		
attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Button elements. When parsing arguments passed to the resetDatamethod the process does not properly validate the existence of an object prior to performing operations on the	Execute Code	17-05-2018	6.8	attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the setAction method of Link objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5569.	ative.com/advisorie s/ZDI-18-349 https://www.foxits oftware.com/suppo rt/security-	Foxit/18-
this vulnerability to execute code	Execute Code	17-05-2018	6.8	attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Button elements. When parsing arguments passed to the resetDatamethod the process does not properly validate the existence of an object prior to performing operations on the object. An attacker can leverage	ative.com/advisorie s/ZDI-18-341 https://www.foxits oftware.com/suppo rt/security-	Foxit/18-

Vulnerability Type(s)	Publish Date	cvsss		Descri	ption & CV	' ID	Referenc	e/Patch	NCIIPC ID
			proc	ess. W	ntext of th as ZDI-C 2018-995 7	AN-5618.			
Execute Code	17-05-2018	6.8	attace code of Fo inter this targe or constant form proceutild prior on the executive of the code of Form proceutild prior on the executive of the code of Form proceutild prior on the code of the code of Form proceutild prior on the code of the code of Form proceutild prior on the code of the code of Form proceutild prior on the code of Form proceutild prior of the code of th	ckers to on vulneral vulneral vulneral vers do de de current code current code code current code	bility in isit a malicemalicious of EXFA When set alue attries not existence of forming of the attracts of t	arbitrary stallations 049. User to exploit that the clous page file. The ithin the Button sting the bute the properly an object operations acker can ability to context of Was ZDI-	https://zer ative.com/s s/ZDI-18-3 https://ww oftware.com rt/security bulletins.pl	advisorie 36 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/38
Execute Code	17-05-2018	6.8	attac code of Fo inter this targe or c spec hand elem attril prop an c oper attac vulne	ckers to on vulneral et must verse the charaction is et must verse the character the control of the control of the character the control of the character the control of the character the control of the control of the character than th	bility in isit a malic malicious rexists worked for the exting the color to point the color to execute to execute to full the color to the	arbitrary stallations 049. User to exploit that the cious page file. The ithin the Button g the title does not istence of erforming bject. An age this ute code	https://zer ative.com/s s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.pl	advisorie 40 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/39
CV Scoring Scale (CV	VSS)	3	4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descrip	otion & CV	ID	Referenc	e/Patch	NCIIPC ID
			CVE	E-ID:CVE-2	018-9956				
Execute Code	17-05-2018	6.8	atta code of F inte this targ or spe han eler attr proj an ope atta vulr und proe	ckers to e on vuln foxit Read eraction is vulneral get must vi open a r cific flaw adling c ments. W ibute the perly valic object pr rations o cker ca nerability er the cor cess. Wa	to execuntext of the	arbitrary tallations 149. User to exploit that the ious page file. The ithin the Button ag the y does not extence of erforming oject. An age this ite code e current AN-5529.	https://zer ative.com/s s/ZDI-18-3 https://ww oftware.com rt/security bulletins.ph	advisorie 38 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/40
Execute Code	17-05-2018	6.8	Th atta code of F inte this targ or spe par attr the exis perfolio this und	is vulneral ckers to e on vulneral caction is vulneral get must viopen a recific flaw sing of Arbute. The lack of forming of ect. An attention vulnerabi	execute erable ins er 9.0.1.10 required to oility in sit a malicious exists wi notation' e issue res of validat an object operations cacker can lity to execute	rs remote arbitrary tallations 049. User to exploit that the ious page file. The thin the s author ults from ing the prior to on the leverage cute code	https://zer ative.com/s s/ZDI-18-3 https://ww oftware.com rt/security bulletins.ph	advisorie 46 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/41
CV Scoring Scale (CV	VSS)	3		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descrij	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			CVI	E-ID:CVE-2	2018-9962				
Execute Code	17-05-2018	6.8	atta cod of I inte this targ or spe par of (from exis per obje this und pro	ckers to be on vulneration is vulneral get must versing of the control of the con	bility allow execute terable inster 9.0.1.10 required to bility in the isit a malicious exists with the name at the ist object operations tacker cantility to execute to the isit of the i	arbitrary tallations 149. User to exploit that the ious page file. The attribute attribute prior to on the leverage cute code e current AN-5568.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.ph	advisorie 48 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/42
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of the pageNum document attribute. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5432. CVE-ID:CVE-2018-9959				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.ph	advisorie 43 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/43
CV Scoring Scale (CV	CV Scoring Scale (CVSS)		4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s) Publish Date	cvsss		Descri	otion & CV	ID	Reference	e/Patch	NCIIPC ID
Execute Code 17-05-2018	6.8	atta cod of l inte this targ or spe pan atta the exis per obj this unc	ackers to le on vulneration is vulneral get must vice open a recific flawersing of ribute. The lack of stence of ect. An attact of the control ocess. Wastence of the control ocess.	execute erable insider 9.0.1.10 required to bility in isit a malici malicious exists wi the receive issue resoft validat an object operations tacker can ility to execute of the	arbitrary tallations 149. User to exploit that the tous page file. The thin the et Field ults from ing the prior to on the leverage cute code e current AN-5434.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.ph	ndvisorie 45 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/44
Execute Code 17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of the textColor Field attribute. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5433. CVE-ID:CVE-2018-9960				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	ndvisorie 44 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/45
Execute Code 17-05-2018	6.8	Thatta	nis vulnera ackers to le on vuln Foxit Read	bility allow execute erable inster 9.0.1.10 required t	rs remote arbitrary tallations 149. User	https://zer ative.com/a s/ZDI-18-3 https://ww	advisorie 53	A-Fox- Foxit/18- 06-18/46
CV Scoring Scale (CVSS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSSS		Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			targ or spec XFA But resu the perf objec this und prod	get must viopen a recific flaw bound ton eler alts from the existence forming of ect. An attitude vulnerabiter the concess. Waster was view was well with the concess.	bility in isit a malicimalicious rexists winders. The helack of vofan objectoperations tacker cantility to execute the as ZDI-C. 2018-9969	ious page file. The thin the thod of ne issue validating on the leverage cute code e current AN-5579.	oftware.con rt/security- bulletins.ph	•	
Execute Code	17-05-2018	6.8	Thi atta code of F inte this targ or spec XFA But resu the perf objecthis und process.	is vulnera ckers to e on vuln foxit Read raction is vulneral get must vi open a n cific flaw resolve ton eler alts from t existence forming of ect. An att vulnerabi er the con cess. Wa	bility allow execute herable inster 9.0.1.10 required to bility in isit a malicious exists with the lack of which of an object operations tacker cantility to execute the execute of the e	rs remote arbitrary tallations 149. User to exploit that the ious page file. The athin the ethod of the issue validating the prior to on the leverage cute code e current AN-5531.	https://zer ative.com/a s/ZDI-18-3. https://ww oftware.cor rt/security- bulletins.ph	advisorie 39 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/47
Execute Code	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the XFA resolveNodes method of				https://zer ative.com/a s/ZDI-18-3: https://ww oftware.com rt/security- bulletins.ph	advisorie 37 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/48
CV Scoring Scale (CVSS)		3	4 4-5 5-6 6-7				7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			Button elements. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5528. CVE-ID:CVE-2018-9953		
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the bitmapDPI attribute of PrintParams objects. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5437. CVE-ID:CVE-2018-1174	https://zerodayiniti ative.com/advisorie s/ZDI-18-312 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/49
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the interactive attribute of PrintParams objects. The issue results from	https://zerodayiniti ative.com/advisorie s/ZDI-18-313 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/50

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5438. CVE-ID:CVE-2018-1175		
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the setTimeOut method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5471. CVE-ID:CVE-2018-9946	https://zerodayiniti ative.com/advisorie s/ZDI-18-330 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/51
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the U3D Node Name buffer. The issue results from the lack of proper validation of user-supplied data which can	https://zerodayiniti ative.com/advisorie s/ZDI-18-390 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/52

CV Scoring Scale (CVSS) Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

5-6

6-7

7-8

8-9

9-10

4-5

3-4

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	I	Descrij	ption &	CV II)	Refer	ence	e/Patch	NCIIPC ID
			allocate leverage other code in process	ed buffge this vulnerant the constant the constant the constant with the constant wi	d past t fer. An a in conju abilities ontext of as ZD 2018-10	attack unctic to e f the e I-CAN	xer can on with execute				
Execute Code Gain Information	17-05-2018	4.3	attacker informations installar 9.0.0.29 required vulneration with executed current installar installar proper prior to can level with executed current installar inst	ers to ation of the state of th	User in	se se vulioxit aterace ploit the bus p file with array the l conjuabilitiontex s ZD	ensitive nerable Reader tion is this target age or . The lack of pointer ttacker unction ies to t of the DI-CAN-	ative.co s/ZDI-1 https://	m/a 8-33 /ww e.con rity-	w.foxits n/suppo	A-Fox- Foxit/18- 06-18/53
Execute Code Gain Information	17-05-2018	4.3	attacker informations and installar such a second required with the second results which	ers to ation ations 9935. ed tability visit a material controller of can rend of	in that malicidalicious exists f U3I ructures the lactuser-susult in an allo	se se vulnoxit aterace ploit the bus p file with D T s. The k of a rea	ensitive nerable Reader tion is this target age or . The hin the exture e issue propered data ad past d data	ative.co s/ZDI-1 https://	m/a 8-39 /ww e.con rity-	w.foxits n/suppo	A-Fox- Foxit/18- 06-18/54
CV Scoring Scale (C	VSS)	3-4	4	4-5	5-6		6-7	7-8		8-9	9-10

Actor Company Compan	Vulnerability Type(s)	Publish Date	cvsss	Descript	ion & CV I	I D	Reference	ce/Patch	NCIIPC ID
attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DataSubBlock structures in GIF images. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an atlacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5490. Execute Code Gain Information Execute Code Gain Information Execute Code Gain Information A-Fox-attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF documents. The issue results from the lack of proper validation of user-supplied data which can result in vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF documents. The issue results from the lack of proper validation of user-supplied data which can result in vulnerability in the context of the context of the context of the current process.				other vulnerab code in the con process. Was	oilities to text of the ZDI-CA	execute current N-5408.			
attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF documents. The issue results from the lack of proper validation of user-supplied data which can result in	Gain	17-05-2018	4.3	This vulnerabil attackers to dinformation installations of 9.0.0.29935. Us required to vulnerability in must visit a mopen a malispecific flaw open a malispecific flaw opensing of structures in issue results in its in its in its interest i	disclose son vulter of the exploit of the end of the of the carry of the execute	s remote sensitive lnerable Reader action is this e target page or e. The chin the abBlock ges. The lack of user-result in of an are. An this in other code in current	ative.com/ s/ZDI-18-3 https://ww oftware.co rt/security	advisorie 317 ww.foxits m/suppo	A-Fox- Foxit/18- 06-18/55
a read past the end of an	Gain	17-05-2018	4.3	attackers to dinformation installations of 9.0.0.29935. Us required to vulnerability in must visit a mopen a mali specific flaw of parsing of PDI issue results for proper validations of the supplied data with the proper validations of the proper valida	disclose so on vulue of Foxit ser intera exploit naticious file icious file icious file icious file icious file icious from the action of which can in the can be seen to be see	sensitive lnerable Reader action is to this e target page or e. The chin the lack of user-result in	ative.com/ s/ZDI-18-3 https://ww oftware.co rt/security	advisorie 334 ww.foxits m/suppo	

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5413. CVE-ID:CVE-2018-9950		
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of Texture Continuation objects in U3D files. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5429. CVE-ID:CVE-2018-9979	https://zerodayiniti ative.com/advisorie s/ZDI-18-377 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/57
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of Texture Image Channels objects in U3D files. The issue results from the lack of proper validation of user-supplied data which can result in	https://zerodayiniti ative.com/advisorie s/ZDI-18-382 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/58

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5495. CVE-ID:CVE-2018-9984		
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of Texture objects in U3D files. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5425. CVE-ID:CVE-2018-9976	https://zerodayiniti ative.com/advisorie s/ZDI-18-374 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/59
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of the U3D Image Index. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an	https://zerodayiniti ative.com/advisorie s/ZDI-18-396 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/60

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5418. CVE-ID:CVE-2018-10486		
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D Clod Progressive Mesh Continuation structures. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5424. CVE-ID:CVE-2018-10492	https://zerodayiniti ative.com/advisorie s/ZDI-18-402 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/61
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files embedded inside PDF documents. The issue results from the lack of proper validation of user-supplied data which can result in	https://zerodayiniti ative.com/advisorie s/ZDI-18-397 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/62

Execute Code Gain Information To State the parage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5419. CVE-ID:CVE-2018-10487 This vulnerability in that the target must visit a malicious page or open a malicious nof context of the contex	Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context process. Was ZDI-CAN-5428. CVE-ID:CVE-2018-9978 Execute Code Gain Information 17-05-2018 Execute Code Gain Information 4.3 This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data which can result in a read past				allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5419.		
attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data which can result in a read past	Gain	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the context process. Was ZDI-CAN-5428.	ative.com/advisorie s/ZDI-18-376 https://www.foxits oftware.com/suppo rt/security-	A-Fox- Foxit/18- 06-18/63
the end of an allocated object. An	Gain	17-05-2018	4.3	attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data	ative.com/advisorie s/ZDI-18-378 https://www.foxits oftware.com/suppo rt/security-	A-Fox- Foxit/18- 06-18/64

Vulnerability Type(s)	Publish Date	CVSSS	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			attacker can conjunction vulnerabilitie the context process. W CVE-ID:CVE-	with s to execut of the as ZDI-C	other e code in current AN-5430.			
Execute Code Gain Information	17-05-2018	4.3	This vulnera attackers to information installations 9.0.0.29935. required to vulnerability must visit a open a machine specific flaw parsing of structures. from the lack of user-supplementallocated dattacker can conjunction vulnerabilitie the context process. Ward CVE-ID:CVE-	disclose on v of Foxit User inter to explo in that the malicious alicious five exists wit U3D Key The issue of proper v lied data w and past the ata struct a leverage with s to execut of the fas ZDI-C	sensitive ulnerable Reader raction is it this ne target page or ile. The ithin the results validation which can end of an ure. An this in other e code in current AN-5399.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.ph	advisorie 89 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/65
Execute Code Gain Information	17-05-2018	4.3	vulnerability must visit a	disclose on v of Foxit User inter to explo in that th malicious alicious fi v exists wi U3D Ligh The issue of proper v lied data w	sensitive ulnerable Reader raction is it this ne target page or ile. The ithin the ht Node e results validation which can	https://www.foxits oftware.com/suppo rt/security- bulletins.php		A-Fox- Foxit/18- 06-18/66
CV Scoring Scale (C	VSS)	3-4	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descr	iption & CV	ID	Reference	e/Patch	NCIIPC ID
			allocated str can leverage with other execute code current pro 5394. CVE-II	e this in co vulnerabi e in the cont cess. Was	njunction lities to ext of the ZDI-CAN-			
Execute Code Gain Information	17-05-2018	4.3	This vulner attackers to information installations 9.0.0.29935. required vulnerability must visit a open a mage of structures. from the lack of user-suppresult in a reallocated structure allocated structure with other execute code current pro 5395. CVE-II	o disclose on v of Foxit User inter to explo in that the malicious halicious halicious for exists wi U3D Mod The issue of proper v olied data w ead past the ructure. An e this in co vulnerabi e in the cont cess. Was	sensitive ulnerable Reader raction is it this he target page or ile. The ithin the el Node e results validation which can end of an attacker njunction lities to ext of the ZDI-CAN-	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security- bulletins.ph	advisorie 86 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/67
Execute Code Gain Information	17-05-2018	4.3	vulnerability must visit a	o disclose on v of Foxit User inter to explo in that the malicious nalicious fi w exists wi U3D Textur objects. The the lack of fuser-supp result in a new	sensitive ulnerable Reader raction is it this ne target page or ile. The ithin the re Coord The issue of proper lied data read past	ative.com/advisorie s/ZDI-18-388 https://www.foxits oftware.com/suppo rt/security- bulletins.php		A-Fox- Foxit/18- 06-18/68
CV Scoring Scale (C	VSS)	3-	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			attacker can conjunction vulnerabilitie the context process. W CVE-ID:CVE-2	with s to execut of the as ZDI-C	other e code in current AN-5397.			
Execute Code Gain Information	17-05-2018	4.3	This vulnera attackers to information installations 9.0.0.29935. required to vulnerability must visit a open a maspecific flaw U3D Texturobject. The is lack of propesupplied data a read pas allocated objeleverage this other vulner code in the coprocess. WCVE-ID:CVE-2	bility allow disclose on violated on viola	rs remote sensitive ulnerable Reader action is it this he target page or le. The thin the Format from the hof userresult in lof an acker cantion with execute e current AN-5409.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security- bulletins.ph	advisorie 92 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/69
Execute Code Gain Information	17-05-2018	4.3	vulnerability must visit a open a m specific flaw Texture Heig issue results	disclose on vo of Foxit User inter to exploi in that th malicious alicious fir exists wit ght structur from the idation of which can t the end	sensitive ulnerable Reader action is it this ne target page or le. The chin U3D ares. The lack of f userresult in l of an	ative.com/advisorie s/ZDI-18-395 https://www.foxits oftware.com/suppo rt/security- bulletins.php		A-Fox- Foxit/18- 06-18/70
CV Scoring Scale (C	VSS)	3-	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			attacker can conjunction vulnerabilitie the context process. W CVE-ID:CVE-	with s to execut of the as ZDI-C	other e code in current AN-5412.			
Execute Code Gain Information	17-05-2018	4.3	vulnerability must visit a open a m specific fla ConvertToPl issue results	disclose on v of Foxit User interato exploin that the malicious file alicious file w exists DF_x86.dll. from the idation of a which can t the end ect. An atta in conjunct abilities to le in the c process. V	sensitive ulnerable Reader action is it this he target page or ile. The within The lack of f user-result in d of an acker can tion with execute ontext of Vas ZDI-	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security bulletins.ph	advisorie 56 vw.foxits m/suppo	A-Fox- Foxit/18- 06-18/71
Execute Code Gain Information	17-05-2018	4.3	vulnerability must visit a	disclose on v of Foxit User interato explo in that the malicious alicious five exists with the lack of user-supplessult in a new ser-supplessult in a new ser-sult in a	sensitive ulnerable Reader action is it this ne target page or ile. The ithin the I'he issue of proper lied data read past	ative.com/advisorie s/ZDI-18-357 https://www.foxits oftware.com/suppo rt/security- bulletins.php		A-Fox- Foxit/18- 06-18/72
CV Scoring Scale (C	VSS)	3	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			attacker car conjunction vulnerabilitie arbitrary coo the current CAN-5758. 9973	with s to le in the c	other execute ontext of Vas ZDI-			
Execute Code Gain Information	17-05-2018	4.3	vulnerability must visit a open a m specific flaw parsing of The issue res	disclose on v of Foxit User interato explo in that the malicious fix v exists wi JPEG2000 ults from the idation of a which can t the end ect. An atta in conjunct cabilities to ontext of the as ZDI-C	sensitive ulnerable Reader action is it this he target page or ile. The ithin the images. he lack of if user-result in d of an acker can tion with execute e current AN-5549.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security bulletins.ph	advisorie 47 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/73
Execute Code Gain Information	17-05-2018	4.3	vulnerability must visit a open a m specific flaw parsing of Maximum R The issue res	disclose on v of Foxit User interato explo in that the malicious alicious five exists with the U3 esolution a ults from the	sensitive ulnerable Reader action is it this ne target page or ile. The ithin the D Final attribute. he lack of of user-	ative.com/advisorie s/ZDI-18-403 https://www.foxits oftware.com/suppo rt/security- bulletins.php		A-Fox- Foxit/18- 06-18/74
CV Scoring Scale (C	VSS)	3	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descrip	otion & CV	ID	Reference	ce/Patch	NCIIPC ID
			a read past allocated obje leverage this other vulnera code in the co process. Wa CVE-ID:CVE-2	ect. An atta in conjunct abilities to ntext of the as ZDI-CA	cker can tion with execute e current AN-5426.			
Execute Code Overflow	17-05-2018	6.8	This vulneral attackers to code on vuln of Foxit Reade interaction is this vulneral target must vior open a respecific flaw parsing of lissue results proper validate user-supplied copying it to a based buffer leverage this execute code to the current CAN-5472.	execute erable inster 9.0.0.299 required to bility in the sit a malicious of the data particular fixed-lengual fixed-lengual fixed-lengual fixed for the culture of the culture for the culture fixed	arbitrary tallations 935. User o exploit that the ous page file. The thin the ges. The lack of length of orior to gth heaptker can oility to ontext of Vas ZDI-	https://zerative.com/ s/ZDI-18-3 https://www.oftware.cort/security bulletins.p	advisorie 331 ww.foxits m/suppo	A-Fox- Foxit/18- 06-18/75
Execute Code Overflow	17-05-2018	6.8	This vulneral attackers to code on vuln of Foxit Reads interaction is this vulneral target must vior open a respecific flaw parsing of The results from validation of supplied data to a fixed-buffer. An att this vulnerabi	execute erable instance of 9.0.0.299 required to oility in sit a malicious for exists with a lack of the lack of the length prior to congth he acker can	arbitrary tallations 35. User o exploit that the ous page file. The thin the The issue of proper of useropying it ap-based leverage	https://zerative.com/ s/ZDI-18-3 https://ww oftware.co rt/security bulletins.p	advisorie 333 ww.foxits m/suppo	A-Fox- Foxit/18- 06-18/76
		3-	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			under the context of the current process. Was ZDI-CAN-5473. CVE-ID:CVE-2018-9949		
Execute Code Overflow	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D Texture Width structures. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5420. CVE-ID:CVE-2018-10488	https://zerodayiniti ative.com/advisorie s/ZDI-18-398 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/77
Execute Code Overflow	17-05-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-5895. CVE-ID:CVE-2018-9974	oftware.com/suppo rt/security-	A-Fox- Foxit/18- 06-18/78

	1						
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Execute Code Overflow	Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID Reference/Patch NCIIPC ID
Execute Code Execute Code Execute Code Code	Execute Code	17-05-2018	6.8	attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D 3DView objects. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5493. CVE-ID:CVE-2018-
Execute Code 24-05-2018 6.8 An issue was discovered in Foxit Reader before 9.1 and PhantomPDF before 9.1. This vulnerability allows remote attackers to execute arbitrary code. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists when rendering U3D images inside of pdf files. The issue results from the lack of proper validation of usersupplied data which can result in a type confusion condition. An attacker can leverage this to execute code in the context of the current process. CVE-ID:CVE-2018-7407 Execute Code 24-05-2018 6.8 An issue was discovered in Foxit Reader before 9.1 and britispic file. The file file for the file file for the file file file. The file file file file file file file fil	PhantompdfRe	ader		
Reader before 9.1 and advisories/src- Phant/1	Execute Code	24-05-2018	6.8	Reader before 9.1 and PhantomPDF before 9.1. This vulnerability allows remote attackers to execute arbitrary code. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists when rendering U3D images inside of pdf files. The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this to execute code in the context of the current process. CVE-ID:CVE-
3-4 4-5 5-6 6-7 7-8 8.0 0.10	Execute Code	24-05-2018	6.8	An issue was discovered in Foxit https://srcincite.io/ A-Fox-
CV Scoring Scale (CVSS)	CV Scoring Scale (C	VSS)	3-4	4 4-5 5-6 6-7 7-8 8-9 9-10

Vulnerability Type(s)	Publish Date	CVSSS	Descr	iption & CV	ID	Referenc	e/Patch	NCIIPC ID	
			PhantomPDF before 9.1. This vulnerability allows remote attackers to execute arbitrary code. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the u3d images inside of a pdf. The issue results from the lack of proper validation of user-supplied data which can result in an array indexing issue. An attacker can leverage this to execute code in the context of the current process. CVE-ID:CVE-2018-7406 6.8 This vulnerability allows remote https://srcincite.io/						
Execute Code	24-05-2018	6.8		nerable instader before sets required to ability in visit a malicious wexists with embeddited data in ger an out-ouffer. An attains vulnerable under the control of the con	arbitrary tallations 9.1 and 9.1. User to exploit that the tous page file. The thin the refer crafted ded u3d the PDF of-bounds acker can bility to context of	https://src advisories/ 2018-0013 https://ww oftware.cor rt/security bulletins.pl	/src- / / / / / / / / / / / / / / / / / / /	A-Fox- Phant/18 06-18/82	
Execute Code	24-05-2018	6.8		lnerable ins ader before F before 9 s required t	https://src advisories/ 2018-0016 https://wv oftware.cor rt/security	/src- / vw.foxits m/suppo	A-Fox- Phant/18 06-18/83		
CV Scoring Scale (C	VSS)	3	4 4-5	5-6	6-7	7-8	8-9	9-10	

Type(s)	Publish Date	CVSSS		Descrij	otion & CV	ID	Reference	e/Patch	NCIIPC ID
Execute Code	24-05-2018	6.8	or spe pro pdf ima the use result allo of Pha interest allo or spe pro pdf ima the use result allo other cod pro than 201 interest allo other cod pro than 201	open a recific flaw ocessing of files with a real cated object and the control of	isit a malici malicious de exists wide past the ferent vuluitation and icious de execute de la comper validation and icious de exists wide past the ferent vuluitation and icious de exists wide past the ferent v	file. The thin the crafted ded u3d alts from dation of nich can end of an acker can tion with execute e current nerability and CVE-VE-2018- To exploit that the lous page file. The thin the crafted ded u3d alts from dation of nich can end of an acker can tion with execute e current nerability and CVE-VE-2018-	https://src.advisories/2018-0015 https://www.oftware.cor.rt/security-bulletins.ph	incite.io/ src- / ww.foxits m/suppo	A-Fox- Phant/18- 06-18/84
Execute Code	24-05-2018	6.8		is vulnera	bility allow execute		https://src	•	A-Fox- Phant/18-
CV Scoring Scale (CV	/SS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code Overflow	24-05-2018	6.8	code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process a different vulnerability than CVE-2018-5679 and CVE-2018-5680. CVE-ID:CVE-2018-5677 This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images. Crafted data in the PDF file can trigger an overflow of a heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process a different vulnerability than CVE-2018-5674 and CVE-2018-5676. CVE-ID:CVE-2018-5676.	https://www.foxits oftware.com/suppo rt/security- bulletins.php https://srcincite.io/ advisories/src- 2018-0012/ https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Phant/18- 06-18/86
		3-	4 4-5 5-6 6-7	7-8 8-9	9-10

CV Scoring Scale (CVSS)

Vulnerability Type(s)	Publish Date	cvsss	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
Execute Code Overflow Execute Code Overflow	24-05-2018	6.8	This vulnera attackers to code on vuln of Foxit Read PhantomPDF interaction is this vulneral target must vor open a specific flaw processing of the can trigged heap-based can leverage execute code the current vulnerability 5674 and CV ID:CVE-2018 This vulneral attackers to code on vuln of Foxit Read PhantomPDF interaction is this vulneral target must vor open a specific flaw processing of the current vulnerability or open a specific flaw processing of the current vulnerability 5676 and CV ID:CVE-2018	bility allow execute herable insider before set than CYE-2018-56 bility allow execute herable insider before before set before before set bility in isit a malicious at than CYE-2018-56 bility allow execute herable insider before set before set before set before set bility in isit a malicious at the cyenter of specially the mbedded data in eran overfouffer. An this vulner under the cyenters at than CYE-2018-56 than CYE-2018-56	rs remote arbitrary tallations 9.1 and 1.1. User to exploit that the tous page file. The thin the remote arbitrary tallations 9.1 and 1.1. User to exploit that the tous page file. The tallations 9.1 and 1.1. User to exploit that the tous page file. The thin the remote arbitrary tallations 9.1 and 1.1. User to exploit that the tous page file. The thin the remote arbitrary tallations 9.1 and 1.1. User to exploit that the tous page file. The thin the remote arbitrary tallations 9.1 and 1.1. User to exploit that the tous page file. The thin the remote arbitrary to context of different vE-2018-	https://srciadvisories/2018-0011/https://www.oftware.com/rt/security-bulletins.ph/	incite.io/src-/w.foxits incite.io/src-/w.foxits in/suppo	A-Fox- Phant/18- 06-18/87 A-Fox- Phant/18- 06-18/88
CV Scoring Scale (CVSS)		3-4	4 4-5 5-6 6-7			7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descrij	ption & CV	ID	Referenc	e/Patch	NCIIPC ID
Hdfgroup								
Hdf5								
DoS	16-05-2018	4.3	A division discovered H5D_btree_d H5Dbtree.c i 1.10.2 library remote denia	ecode_key n the HE y. It could ll of servic	in in DF HDF5 allow a ce attack.	https://git Twi1ight/f pocs/tree/ df5	uzzing-	A-Hdf- Hdf5/18- 06-18/89
DoS	16-05-2018	4.3	A division discovered in H5Dchunk.c 1.10.2 library remote denia	H5D_chui in the HI 7. It could Il of servic	nk_init in DF HDF5 allow a ce attack.	https://git Twi1ight/f pocs/tree/ df5	uzzing-	A-Hdf- Hdf5/18- 06-18/90
DoS	16-05-2018	4.3	A NULL poin discovered H50_chunk_o H50cache.c i 1.10.2 library remote denia CVE-ID:CVE-2	deserialize in the HI 7. It could Il of servic	in in DF HDF5 allow a ce attack.	https://git Twi1ight/f pocs/tree/ df5	uzzing-	A-Hdf- Hdf5/18- 06-18/91
DoS	16-05-2018	5.8	A out of discovered H50_fill_new_H50_fill_old_din the HDF HI could allow service or infattack. CVE-II	decode lecode in OF5 1.10.2 a remote ormation d	in and H5Ofill.c library. It denial of lisclosure	https://git Twi1ight/f pocs/tree/ df5	uzzing-	A-Hdf- Hdf5/18- 06-18/92
DoS	16-05-2018	5.8	attack. CVE-ID:CVE-2018-11206 A out of bounds read was discovered in H5VM_memcpyvv in H5VM.c in the HDF HDF5 1.10.2 library. It could allow a remote denial of service or information disclosure attack. CVE-ID:CVE-2018-11205		A out of bounds read was discovered in H5VM_memcpyvv in H5VM.c in the HDF HDF5 1.10.2 library. It could allow a remote denial of service or information disclosure attack.		hub.com/ uzzing- master/h	A-Hdf- Hdf5/18- 06-18/93
CV Scoring Scale (C	VSS)	3	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss		Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
IBM									
Spectrum Vir SoftwareStorw				V5000 Sof	twareStor	wize V700	alize Softw O Software	areStorw/	ize V3500
CSRF	17-05-2018	6.8	Storand 6.1 7.6 and cross cou execuna from trus	rwize IBM IBM Flas 6.2 6.3 6.4 7.6.1 7.7 8.1.1) ss-site req ld allow cute uthorized n a user	malicious actions tra that the X-Force	Virtualize roducts (3 7.4 7.5 7.8.1 8.1 rable to ry which ocker to and ansmitted website	https://exc orce.ibmclo vulnerabilit 474	oud.com/	A-IBM- Spect/18- 06-18/94
DoS	17-05-2018	6.5	Stor and 6.1 7.6 and auth syst acce or c	rwize IBM IBM Flas 6.2 6.3 6.4 7.6.1 7.7 8.1.1) henticated tem files these to including a dorce ID		Virtualize roducts (37.47.57.8.18.1 llow an access not have string files vice. IBM	https://exc orce.ibmclc vulnerabilit 363	oud.com/	A-IBM- Spect/18- 06-18/95
Gain Information	17-05-2018	3.5	IBI Stor and 6.1 7.6 and autl priv inte	M SAN Vol rwize IBM IBM Flas 6.2 6.3 6.4 7.6.1 7.7 8.1.1) henticated vate key ercepting (user to o which cou GUI commu I X-Force	Virtualize roducts (.3 7.4 7.5 7.8.1 8.1 llow an btain the lld make nications	orce.ibmcloud.com/ vulnerabilities/140 396		A-IBM- Spect/18- 06-18/96
Gain Information	17-05-2018	4	Stor and	rwize IBM IBM Flas	ume Contr Spectrum V hSystem p 4 7.1 7.2 7.	orce.ibmclo	https://exchange.xf orce.ibmcloud.com/ vulnerabilities/140		
CV Scoring Scale (CV	VSS)	3	4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Des	scription & CV	'ID	Reference	e/Patch	NCIIPC ID
V			and 8.1. authentica sensitive should no	ated user to information of thave author MX-Force	llow an obtain that they			
Gain Information	17-05-2018	5	IBM SAN Storwize I and IBM I 6.1 6.2 6.3 7.6 7.6.1 and 8.1.1 could allo attacker to	Volume Contr BM Spectrum FlashSystem p 3 6.4 7.1 7.2 7 7.7 7.7.1 7.8 web handler w an unauth o read arbitran n. IBM X-Force	Virtualize roducts (.3 7.4 7.5 7.8.1 8.1 /DLSnap lenticated by files on	https://exc orce.ibmclc vulnerabilit 566	oud.com/	A-IBM- Spect/18- 06-18/98
Gain Information	17-05-2018	5	Storwize I and IBM I 6.1 6.2 6.3 7.6 7.6.1 and 8. /Downloa authentica files from	Volume Control BM Spectrum FlashSystem p 3 6.4 7.1 7.2 7 7.7 7.7.1 7.8 1.1) web dFile does not ation to read the system of the s	Virtualize roducts (.3 7.4 7.5 7.8.1 8.1 handler of require arbitrary IBM X-	https://exc orce.ibmclc vulnerabilit 473	A-IBM- Spect/18- 06-18/99	
NA	17-05-2018	3.5	IBM SAN Storwize I and IBM (6.1 6.2 6. 7.6 7.6.1 and 8.1.1 expected algorithm attacker sensitive	Volume Contr BM Spectrum FlashSystem .3 6.4 7.1 7.2 7 7.7 7.7.1 7.8 1) use weal cryp s that could to decrypt information. D CVE-ID:C	Virtualize products 7.3 7.4 7.5 7.8.1 8.1 ser than tographic allow an highly IBM X-	https://exc orce.ibmclc vulnerabilit 397	oud.com/	A-IBM- Spect/18- 06- 18/100
NA	17-05-2018	4	IBM SAN Storwize I and IBM	hange.xf oud.com/ ties/140	A-IBM- Spect/18- 06-			
CV Scoring Scale (C	VSS)	3	4 4-:	5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) could allow an authenticated user to access system files they should not have access to some of which could contain account credentials. IBM X-Force ID CVE-ID:CVE-2018-1463	368	18/101
XSS	17-05-2018	3.5	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID CVE-ID:CVE-2018-1461	https://exchange.xf orce.ibmcloud.com/ vulnerabilities/140 362	A-IBM- Spect/18- 06- 18/102
IJG Libjpeg					
DoS	16-05-2018	4.3	An issue was discovered in libjpeg 9a. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted file. CVE-ID:CVE-2018-11212	https://github.com/ ChijinZ/security_ad visories/tree/maste r/libjpeg-v9a	A-IJG- Libjp/18- 06- 18/103
DoS	16-05-2018	4.3	An issue was discovered in libjpeg 9a. The get_text_gray_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file. CVE-ID:CVE-2018-11213	https://github.com/ ChijinZ/security_ad visories/tree/maste r/libjpeg-v9a	A-IJG- Libjp/18- 06- 18/104
DoS	16-05-2018	4.3	An issue was discovered in libjpeg 9a. The get_text_rgb_row function in rdppm.c allows	https://github.com/ ChijinZ/security_ad visories/tree/maste	A-IJG- Libjp/18- 06-
CV Scoring Scale (CV	/SS)	3	4 4-5 5-6 6-7	7-8 8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			remote atta denial of ser fault) via a ID:CVE-2018	crafted fi	nentation	r/libjpeg-v	Эа	18/105
Ilias								
Ilias NA	17-05-2018	5.8	ILIAS 5.1.x 5	2 v and 5 3	v hefore	https://ww	nw iliae d	A-Ili-
IVA	17-03-2016	5.0	5.3.5 redirect a third-par return_to_url ID:CVE-2018	s a logged-i ty site paramete	n user to via the	e/docu/got rget=st_229 github.com eLearning/ mmit/01a2 dddf1da59d 063797348	o.php?ta Phttps:// /ILIAS- ILIAS/co 4cf04fe8 ca49758	Ilias/18- 06- 18/106
XSS	17-05-2018	4.3	Services/COP PCSourceCod 5.2.x and 5.3 XSS. CVE-ID:0	e.php in IL 3.x before !	IAS 5.1.x 5.3.5 has	https://ww e/docu/got rget=st_229 github.com eLearning/ mmit/7959 b981976b6 cf95060392	o.php?ta Phttps:// /ILIAS- ILIAS/co !485406e !4fee363	A-Ili- Ilias/18- 06- 18/107
XSS	17-05-2018	4.3	Services/Feed ternalFeedIte 5.2.x and 5.3 XSS via a l ID:CVE-2018	m.php in IL 3.x before ! ink attribu	IAS 5.1.x 5.3.5 has	https://ww e/docu/got rget=st_229 github.com eLearning/ mmit/ff9bf dbffe82871 7038c00d7	o.php?ta Phttps:// /ILIAS- ILIAS/co 29858f2 1a6f8bf3	A-Ili- Ilias/18- 06- 18/108
XSS	17-05-2018	4.3	The RSS sub 5.2.x and 5.3 XSS via Services/Feed ternalFeedIte 2018-11118	B.x before ! a U ds/classes/c m.php. CVE	5.3.5 has RI to class.ilEx	https://github.com/ ILIAS- eLearning/ILIAS/co mmit/6b2217c31b6 974788a5c7874134 54475687b44bb https://www.ilias.d e/docu/goto.php?ta rget=st_229https:// github.com/ILIAS- eLearning/ILIAS/co mmit/d0dcad1b1e7		A-Ili- Ilias/18- 06- 18/109
CV Scoring Scale (C	VSS)	3-4	4 4-5	5-6	6-7	7-8	8-9	9-10

Imagemagick	Vulnerability Type(s)	Publish Date	cvsss	Descr	iption & CV	ID	Reference	e/Patch	NCIIPC ID
DoS 18-05-2018 4.3 In ImageMagick 7.0.7-16 Q16 Magick/issues/918 Magick/	Jr · (-)								
DoS	Imagemagick								
NA 31-05-2018 As In ImageMagick / Image Image/18 Ima	Imagemagick								
X86_64 2018-01-24 there is a heap-based buffer over-read in ReadSUNImage in coders/sun. which allows attackers to cause a denial of service (application crash in SetGrayscaleImage in MagickCore/quantize.c) via a crafted SUN image file. CVE-ID:CVE-2018-11251	DoS	18-05-2018	4.3	x86_64 201 use-after-fre ReadOneMN coders/png.c attackers to service via a file that is MngInfoDisc	7-12-25 the e GImage c which cause a carafted MM mishandle ardObject c	ere is a in in allows denial of IG image d in an	ImageMag	ick/Image	Image/18 -06-
theReadMATImage function in coders/mat.c allows attackers to cause a use after free via a crafted file. CVE-ID:CVE-2018-11624 Overflow 31-05-2018 6.8 In ImageMagick 7.0.7-37 Q16SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer overread via a crafted file. CVE-ID:CVE-2018-11625 Microsoft Office For Mac Exec Code 23-05-2018 9.3 A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly validate XML content aka "Microsoft CVE-2018-8176 Image/18 -06-18/112 Microsoft Office For Mac Exec Code 23-05-2018 9.3 A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly validate XML content aka "Microsoft CVE-2018-8176 Image/18 -06-18/112 A-Image/18 -06-18/112 A-Image/18 -06-18/112 A-Image/18 -06-18/113 A-Image/18 -06-	DoS Overflow	18-05-2018	4.3	x86_64 201 heap-based ReadSUNIma which allows denial of crash in So MagickCore/ crafted SUN	8-01-24 the buffer over age in codes attackers to service (apetGrayscale (quantize.c)	ere is a read in ers/sun.c o cause a plication mage in via a	com/3681 1/https:// m/ImageM ageMagick 56https:// an.org/del announce/	github.co lagick/Im /issues/9 lists.debi pian-lts- /2018/05	Image/18 -06-
Q16SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer overread via a crafted file. CVE-ID:CVE-2018-11625 Microsoft Office For Mac Exec Code 23-05-2018 9.3 A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly validate software fails to properly validate XML content aka "Microsoft CVE-2018-8176 Image/18 1/https://github.co m/ImageMagick/Im ageMagick/issues/1 156 8-Microsoft US/security-guidance/advisory/CVE-2018-8176	NA	31-05-2018	6.8	theReadMAT coders/mat.c cause a use a	Timage fun c allows atta after free via	ction in ackers to a crafted	ImageMag Magick/iss	ick/Image	Image/18 -06-
Exec Code 23-05-2018 9.3 A remote code execution https://portal.msrc. vulnerability exists in Microsoft microsoft.com/en-PowerPoint software when the software fails to properly validate guidance/advisory/XML content aka "Microsoft CVE-2018-8176 06-18/114	Overflow	31-05-2018	6.8	Q16SetGrays quantize.c fil cause a hea read via a	scaleImage le allows att p-based buf crafted fi	in the ackers to fer over-	com/3681 1/https:// m/ImageMageMageMageMageK	- github.co lagick/Im	Image/18 -06-
Exec Code 23-05-2018 9.3 A remote code execution https://portal.msrc. vulnerability exists in Microsoft microsoft.com/en- PowerPoint software when the software fails to properly validate guidance/advisory/ XML content aka "Microsoft CVE-2018-8176 18/114	Microsoft								
vulnerability exists in Microsoft microsoft.com/en- PowerPoint software when the software fails to properly validate guidance/advisory/ XML content aka "Microsoft CVE-2018-8176 344 45 56 67 78 78 89 89 818	Office For Mac								
3-4 4-5 5-6 6-7 7-8 8-9 9-10		23-05-2018	9.3	vulnerability exists in Microsoft microsoft.com/en- PowerPoint software when the software fails to properly validate guidance/advisory/					
CV Scoring Scale (CVSS)	CV Scoring Scale (C)	VSS)	3	4 4-5	5-6	6-7	7-8	8-9	9-10

Injection; XSS- Cross Site Scripting;

PowerPoint Remote Code Execution Vulnerability." This articles The Podofo	Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID						
DoS				Execution Vulnerability." This affects Microsoft Office. CVE-								
DoS												
PoDoFo 0.9.5. The function PdfPageCVE-ID:CVE-2018- 11255		10.05.2010	4.0	A : 1: 1 :	1 //1 :11 1	4 D 1						
PoDoFo 0.9.5. There is an Excession in the PdfPagesTreeCVE-ID:CVE-2018- 11254	Dos	18-05-2018	4.3	PoDoFo 0.9.5. The function PdfPage CVE-ID:CVE-2018-	hat.com/show_bug.c	Podof/18- 06-						
NA 22-05-2018 S In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the DNS dissector could crash. This was addressed in epan/dissectors/packet-dns.c by avoiding a NULL pointer dereference for an empty name in an SRV record. CVE-ID:CVE-2018-11356 CVE-ID:CVE-2018-11356 CVE-ID:CVE-2018-11356 CVE-ID:CVE-2018-11356 CVE-ID:CVE-2018-11356 CVE-ID:CVE-2018-11356 CVE-ID:CVE-2018-11356 CVE-ID:CVE-2018-11357 CVE-ID:CVE-2	DoS	18-05-2018	4.3	PoDoFo 0.9.5. There is an Excessive Recursion in the PdfPagesTree CVE-ID:CVE-2018-	hat.com/show_bug.c	Podof/18- 06-						
NA 22-05-2018												
and 2.2.0 to 2.2.14 the DNS dissector could crash. This was addressed in epan/dissectors/packet-dns.c by avoiding a NULL pointer dereference for an empty name in an SRV record. CVE-ID:CVE-2018-11356 NA 22-05-2018 In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the LTP dissector and other dissectors could consume excessive memory. This was addressed in epan/tvbuff.c by rejecting negative lengths. CVE-ID:CVE-2018-11357 NA 24 45 56 67 7.8 8.8 9.0 0.00					1.							
and 2.2.0 to 2.2.14 the LTP dissector and other dissectors could consume excessive memory. This was addressed in epan/tvbuff.c by rejecting negative lengths. CVE-ID:CVE-2018-11357 and 2.2.0 to 2.2.14 the LTP hark.org/security/w npa-sec-2018-28.html bark.org/security/w npa-sec-2018-28.html color npa-sec-2018-28.html https://bugs.wiresh ark.org/bugzilla/sh ow_bug.cgi?id=1467				and 2.2.0 to 2.2.14 the DNS dissector could crash. This was addressed in epan/dissectors/packet-dns.c by avoiding a NULL pointer dereference for an empty name in an SRV record. CVE-ID:CVE-2018-11356	hark.org/security/w npa-sec-2018- 29.html https://bugs.wiresh ark.org/bugzilla/sh ow_bug.cgi?id=1468 1 https://code.wiresh ark.org/review/git web?p=wireshark.gi t;a=commit;h=4425 716ddba99374749b d033d9bc0f4add2fb 973	Wires/18 -06- 18/117						
CV Scoring Scale (CVSS) 3-4 4-5 5-6 6-7 7-8 8-9 9-10	NA	22-05-2018	5	and 2.2.0 to 2.2.14 the LTP dissector and other dissectors could consume excessive memory. This was addressed in epan/tvbuff.c by rejecting negative lengths. CVE-ID:CVE-	hark.org/security/w npa-sec-2018- 28.html https://bugs.wiresh ark.org/bugzilla/sh ow_bug.cgi?id=1467	Wires/18 -06-						
(CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10						

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
				https://code.wiresh ark.org/review/git web?p=wireshark.gi t;a=commit;h=ab8a 33ef083b9732c891 17747a83a905a676 faf6	
NA	22-05-2018	5	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the Q.931 dissector could crash. This was addressed in epan/dissectors/packet-q931.c by avoiding a use-after-free after a malformed packet prevented certain cleanup. CVE-ID:CVE-2018-11358	https://www.wires hark.org/security/w npa-sec-2018- 31.html https://www.debia n.org/security/201 8/dsa-4217 https://code.wiresh ark.org/review/git web?p=wireshark.gi t;a=commit;h=ccb1a c3c8cec47fbbbf2e8 0ced80644005c652 52 https://lists.debian. org/debian-lts- announce/2018/05 /msg00019.htmlhtt	A-Wir- Wires/18 -06- 18/119
				ps://bugs.wireshark .org/bugzilla/show_ bug.cgi?id=14689	
NA	22-05-2018	5	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the RRC dissector and other dissectors could crash. This was addressed in epan/proto.c by avoiding a NULL pointer dereference. CVE-ID:CVE-2018-11359	https://www.wires hark.org/security/w npa-sec-2018- 33.html https://bugs.wiresh ark.org/bugzilla/sh ow_bug.cgi?id=1470 3 https://code.wiresh	A-Wir- Wires/18 -06- 18/120
		3-	4 4-5 5-6 6-7	7-8 8-9	9-10

CV Scoring Scale (CVSS)

Vulnerability Type(s)	Publish Date	cvsss		Descrij	ption & CV	ID	Referenc	e/Patch	NCIIPC ID
				ark.org/review/git web?p=wireshark.gi t;a=commit;h=beaeb e91b14564fb9f86f0 726bab0992787272 1b				eshark.gi t;h=beaeb lfb9f86f0	
NA	22-05-2018	5	In Wireshark2.6.0 the IEEE 1905.1a dissector could crash. This was addressed in epan/dissectors/packetieee1905.c by making a certain correction to string handling. CVE-ID:CVE-2018-11354				https://ww hark.org/so npa-sec-20 26.html https://bus ark.org/bu ow_bug.cgi 7 https://coo ark.org/rev web?p=wir t;a=commit 7a4a43438 75ebb1066 251c	gs.wiresh gzilla/sh ?id=1464 de.wiresh view/git reshark.gi t;h=cb51	A-Wir- Wires/18 -06- 18/121
Overflow	22-05-2018	5	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the GSM A DTAP dissector could crash. This was addressed in epan/dissectors/packet-gsm_dtap.c by fixing an off-by-one error that caused a buffer overflow. CVE-ID:CVE-2018-11360				https://bugark.org/bugark.org/bugow_bug.cgighttps://cohark.org/reweb?p=wirt;a=commitg36c51f83ag24e8ee3a6b24bhttps:ebian.org/s2018/dsag217https:wireshark.org/sylvynpa-s30.html	gzilla/sh ?id=1468 ode.wires eview/git reshark.gi t;h=a55b 7b96808 ce8429a //www.d security/	A-Wir- Wires/18 -06- 18/122
Overflow	22-05-2018	5	and dist	In Wireshark2.6.0 2.4.0 to 2.4.6 https://www.wireand 2.2.0 to 2.2.14 the LDSS hark.org/security/dissector could crash. This was addressed in epan/dissectors/packet-ldss.c by https://www.debi			ecurity/w 18-	A-Wir- Wires/18 -06- 18/123	
CV Scoring Scale (CVSS)		3-	•	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID
			avoiding a buffer over-read upon encountering a missing '0' character. CVE-ID:CVE-2018-11362	n.org/security/201 8/dsa-4217 https://lists.debian. org/debian-lts- announce/2018/05 /msg00019.html https://bugs.wiresh ark.org/bugzilla/sh ow_bug.cgi?id=1461 5 https://code.wiresh ark.org/review/git web?p=wireshark.gi t;a=commit;h=f1770 08b04a530640de83 5ca878892e58b826 d58	
Overflow	22-05-2018	5	In Wireshark2.6.0 the IEEE 802.11 protocol dissector could crash. This was addressed in epan/crypt/dot11decrypt.c by avoiding a buffer overflow during FTE processing in Dot11DecryptTDLSDeriveKey. CVE-ID:CVE-2018-11361	https://www.wires hark.org/security/w npa-sec-2018- 32.html https://bugs.wiresh ark.org/bugzilla/sh ow_bug.cgi?id=1468 6 https://code.wiresh ark.org/review/git web?p=wireshark.gi t;a=commit;h=1b52f 9929238ce3948ec9 24ae4f9456b5e9df5 58	A-Wir- Wires/18 -06- 18/124

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvsss	Descrip	otion & CV l	D	Reference	e/Patch	NCIIPC ID
Overflow	22-05-2018	5	In Wireshandissector couladdressed epan/dissecto avoiding a b packet statu	ers/packet-r uffer overf us chunks	his was in tcp.c by low for	https://wv hark.org/s npa-sec-20 27.html https://bu ark.org/bu ow_bug.cgi 3 https://co ark.org/re web?p=win t;a=commi 7a5fd2c54 aca3b3647	gs.wiresh igzilla/sh i?id=1467 de.wiresh view/git reshark.gi t;h=99d2 0f837154	A-Wir- Wires/18 -06- 18/125
			0 .: 0			3		
CanonicalDohi	anImagemagicl		onOperating S	ystem (Ap)	plication	08)		
	nagemagickUbi		X					
DoS	18-05-2018	7.1	In ImageMa x86_64 2017 loop vulnerab the function coders/miff.c attackers to service (CPU crafted MIFF ID:CVE-2017-	-12-22 an oility was f ReadMIFFI which cause a d exhaustion image fil	infinite found in mage in allows enial of a) via a	https://git ImageMag: Magick/iss https://lis org/debiar announce/ /msg0001 https://us com/3681	ick/Image sues/911 ts.debian. n-lts- /2018/05 2.html n.ubuntu.	A-Can- Debia/18- 06- 18/126
DoS	18-05-2018	7.1	In ImageMa x86_64 2017 loop vulneral the function coders/txt.c attackers to service (CPU crafted image mishandled GetImageInder ID:CVE-2017-	gick 7.0.712-22 an oility was feadTXTIr which cause a dexhaustion ge file taxInList cal	infinite found in mage in allows enial of allowing athat is	https://git ImageMag Magick/iss https://us com/3681 https://lis org/debiar announce/ /msg0001	chub.com/ ick/Image sues/910 n.ubuntu. -1/ ts.debian. n-lts- /2018/05	A-Can- Debia/18- 06- 18/127
CV Scoring Scale (CVSS)		3-4	4 4-5	5-6	6-7	7-8	8-9	9-10
	(s): CSRF-Cross Site	Request For	gery; Dir. TravDir	ectory Traver	sal; DoS-Dei	nial of Service;	NA- Not Appli	cable; Sql-SQL

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	cvsss	Description & CV ID	Reference/Patch	NCIIPC ID							
			Operatingt System (OS)									
Microsoft												
Windows 10W	Windows 10Windows 7Windows 8.1Windows Rt 8.1Windows Server 2008Windows Server 2012Windows											
Server 2016												
Overflow	14-06-2018	7.6	A memory corruption	https://portal.msrc.	O-Mic-							
Memory			vulnerability exists when	microsoft.com/en-	Windo/18							
Corruption			Windows Media Foundation	US/security-	-06-							
			improperly handles objects in memory aka "Media Foundation	, , ,	18/128							
			Memory Corruption									
			Vulnerability." This affects									
			Windows 7 Windows Server									
			2012 R2 Windows RT 8.1									
			Windows Server 2012 Windows									
			8.1 Windows Server 2016									
			Windows Server 2008 R2									
			Windows 10 Windows 10									
			Servers. CVE-ID:CVE-2018-8251									
Windows 10Wi	indows Server 2	2016										
NA	14-06-2018	7.2	An elevation of privilege vulnerability exists in Windows	https://portal.msrc. microsoft.com/en-	O-Mic- Windo/18							
			when the Win32k component	, ,	-06-							
			fails to properly handle objects in	guidance/advisory/	18/129							
			memory aka "Win32k Elevation	CVE-2018-8233								
			of Privilege Vulnerability." This									
			affects Windows 10 Windows 10									
			Servers. CVE-ID:CVE-2018-8233									

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
g - 1 (- 1 - 1)							