(1)	National C	ritical	Information Infrastructu	re Protection Ce	ntre
CV S	coring Scale	: 3-10	<i>CVE Report</i> 15 May –15 Jun 2018	Vol. 0	5 No.11
Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Application		.
Dolibarr					
Dolibarr					
XSS	22-05-2018	4.3	Cross-site scripting (XSS) vulnerability in Dolibarr before 7.0.2 allows remote attackers to inject arbitrary web script or HTML via the foruserlogin parameter to adherents/cartes/carte.php. CVE- ID:CVE-2018-10095	https://sysdream.co m/news/lab/2018- 05-21-cve-2018- 10095-dolibarr-xss- injection- vulnerability/ https://github.com/ Dolibarr/dolibarr/c ommit/1dc466e1fb 687cfe647de4af891 720419823ed56 https://github.com/ Dolibarr/dolibarr/b lob/7.0.2/ChangeLo g	A-Dol- Dolib/18- 06-18/1
Foxitsoftware				0	
Foxit Reader					
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. 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 data structure. An attacker can leverage this in conjunction with other	https://zerodayiniti ative.com/advisorie s/ZDI-18-381 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/2

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Red Injection; XSS- Cross Site Scripting;	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Den	ial of Service; I	NA- Not Applic	able; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSSS		Descrij	otion & CV	ID	Referenc	e/Patch	NCIIPC ID
			the o proces	context ss. Wa	s to execut of the as ZDI-C. 2018-9983	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/s s/ZDI-18-3 https://ww oftware.con rt/security bulletins.pl	advisorie 28 vw.foxits m/suppo -	A-Fox- Foxit/18- 06-18/3
Execute Code	17-05-2018	6.8	This v attacke code of of Fox interact this v target or op specif AFSim The iss validat object operatt attacke vulner under proces	vulnera ers to on vuln it Reado ction is vulneral must vi en a r ic flaw ple_Ca sue resu ting th prion tions o er ca rability the con ss. Wa	bility allow execute erable ins er 9.0.0.299 required to bility in sit a malici- malicious exists wi lculate alts from the e existence to pera- to execu- n the of n levera- to execu-	vs remote arbitrary tallations 935. User to exploit that the ious page file. The ithin the method. he lack of the of an erforming oject. An ge this ite code e current AN-5491.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.con rt/security bulletins.pl	advisorie 18 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/4
CV Scoring Scale (C)	V(CC)	3-4	4	4-5	5-6	6-7	7-8	8-9	9-10

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

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

 Visit and the state of th

Vulnerability Type(s)	Publish Date	CVSSS		Descrip	tion & CV	ID	Reference	e/Patch	NCIIPC ID
Execute Code	17-05-2018	6.8	atta cod of I inte this targ or spe get res the per obj this unc pro	ackers to le on vuln Foxit Reade eraction is s vulnerat get must vi open a m cific flaw Field me ults from th existence of forming of ect. An att s vulnerabil der the con bcess. Wa E-ID:CVE-2	execute erable ins er 9.0.0.299 required to bility in sit a malici- nalicious exists wi ethod. The lack of wo of an objecto perations acker can lity to execu- text of the as ZDI-C.	arbitrary tallations 35. User to exploit that the ious page file. The thin the re issue validating t prior to on the leverage cute code e current AN-5382.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security- bulletins.ph	advisorie 29 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/5
Execute Code	17-05-2018	6.8	CVE-ID:CVE-2018-9945 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. CVE-ID:CVE-2018-9951				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	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			vs remote arbitrary tallations 935. User to exploit	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security	advisorie 23 vw.foxits n/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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/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 handling of layout elements. 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-5373. CVE-ID:CVE-2018-9939 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 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- 9938	bulletins.php https://zerodayiniti ative.com/advisorie s/ZDI-18-322 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/8
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 the addAnnot	https://zerodayiniti ative.com/advisorie s/ZDI-18-315 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/9

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10			
Vulnerability Type(s): CSRF-Cross Site Ree	Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Type(s) Execute Code	17-05-2018	6.8	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-5488. CVE-ID:CVE-2018-1177 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 addField 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	https://zerodayiniti ative.com/advisorie s/ZDI-18-316	A-Fox- Foxit/18- 06-18/10
			this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5489. CVE-ID:CVE-2018-1178		
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 the layout sheet attribute. The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can	ative.com/advisorie s/ZDI-18-324 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/11

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Ree	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Deni	ial of Service; N	NA- Not Applica	able; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			leverage this vulnerability to execute code under the context of the current process. Was ZDI- CAN-5374. CVE-ID:CVE-2018- 9940		
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 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	https://zerodayiniti ative.com/advisorie s/ZDI-18-327 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/12
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 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

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10			
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL										
Injection; XSS- Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSSS	Descr	ription & CV	ID	Reference	e/Patch	NCIIPC ID
			CAN-5375. 9941	CVE-ID:CV	/E-2018-			
Execute Code	17-05-2018	6.8	attackers to code on vui of Foxit Rea interaction if this vulner target must or open a specific flay handling of method. The the lack of user-supplie result in condition. leverage th	Inerable ins der 9.0.0.299 is required t ability in visit a malici malicious w exists wi f the record he issue resu proper valid ed data wh a type of An attack his vulneral e under the o	arbitrary tallations 035. User to exploit that the ous page file. The thin the remove alts from dation of nich can confusion ker 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 26 vw.foxits n/suppo	A-Fox- Foxit/18- 06-18/14
Execute Code	17-05-2018	6.8	This vulner attackers to code on vul of Foxit Rea interaction is this vulner target must or open a specific flay handling borderColo issue result validating to operations attacker of vulnerability under the co process. V	ability in visit a malici malicious w exists wi of the r attribut as from the che existence or to pe on the ob can levera y to execu-	arbitrary tallations 035. User to exploit that the ous page file. The thin the XFA ce. The lack of the of an erforming oject. An ge this the code e current AN-5436.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	advisorie 11 vw.foxits n/suppo -	A-Fox- Foxit/18- 06-18/15
CV Scoring Scale (C)		3-4	4 4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQLInjection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
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 ePub files. The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5442. CVE-ID:CVE-2018-1176	https://zerodayiniti ative.com/advisorie s/ZDI-18-314 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/16
Execute Code	17-05-2018	6.8	CVE-ID:CVE-2018-1176 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 field elements. 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-5370. CVE-ID:CVE-2018-9936	https://zerodayiniti ative.com/advisorie s/ZDI-18-320 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/17
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	https://zerodayiniti ative.com/advisorie s/ZDI-18-400 https://www.foxits	A-Fox- Foxit/18- 06-18/18

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

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

Vulnerability Type(s)	Publish Date	CVSSS	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			embedded in issue results	isit a malic malicious exists wi f JPEG from the dation of which can cess past th data struc n levera to execu ntext of the as ZDI-C	ious page file. The ithin the images files. The e lack of f user- result in he end of cture. An ge this ite code e current AN-5422.	oftware.cor rt/security- bulletins.ph	-	
Execute Code	17-05-2018	6.8	This vulnera attackers to code on vulr of Foxit Read interaction is this vulnera target must v or open a specific flaw	bility allow execute nerable ins er 9.0.0.29 required t bility in isit a malici- malicious exists wi Modifier 3D files. The lack of wo of an object operations tacker can ility to execute ntext of the as ZDI-C.	vs remote arbitrary tallations 935. User to exploit that the ious page file. The ithin the c Chain The issue validating t prior to on the leverage cute code e current AN-5427.	https://zer ative.com/a s/ZDI-18-3 https://ww oftware.cor rt/security- bulletins.ph	A-Fox- Foxit/18- 06-18/19	
Execute Code	17-05-2018	6.8	This vulnera attackers to code on vulr of Foxit Read interaction is this vulnera target must v or open a	bility allow execute ierable ins er 9.0.0.29 required t bility in isit a malic	vs remote arbitrary tallations 935. User to exploit that the ious page	https://zer ative.com/a s/ZDI-18-4 https://ww oftware.com rt/security- bulletins.ph	A-Fox- Foxit/18- 06-18/20	
CV Scoring Scale (CV	3-	4 4-5	5-6	6-7	7-8	8-9	9-10	

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			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 a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5586. CVE-ID:CVE-2018-10495		
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 subform elements. 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-5371. CVE-ID:CVE-2018-9937	https://zerodayiniti ative.com/advisorie s/ZDI-18-321 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/21
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 the Texture Width in U3D files. The issue results from the lack of proper validation of user-supplied data which can	oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/22

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									

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 attacker 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 past 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	https://zerodayiniti 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 can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to	1 //	A-Fox- Foxit/18- 06-18/24

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								
Injection; XSS- Cross Site Scripting;								

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			execute code under the context of the current process. Was ZDI- CAN-5396. CVE-ID:CVE-2018- 10477		
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 CLOD Base Mesh Continuation structures. The issue results from the lack of proper validation of user- supplied data which can result in a write past 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-5392. CVE-ID:CVE-2018- 10473	https://zerodayiniti ative.com/advisorie s/ZDI-18-383 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/25
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 Clod Progressive Mesh Declaration structures . The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code	https://zerodayiniti ative.com/advisorie s/ZDI-18-399 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/26

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								

Vulnerability Type(s)	Publish Date	CVSSS	Descrij	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			under the comprocess. War CVE-ID:CVE-2	as ZDI-C	AN-5421.			
Execute Code	17-05-2018	6.8	Progressive issue results	execute lerable ins er 9.0.0.299 required t bility in isit a malici malicious f exists wi of U3D Mesh objection from the dation o which can be the end ect. An attants under the c	arbitrary tallations 35. User to exploit that the ious page file. The thin the Clod ects. The lack of f user- result in d of an ocker 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				https://zer ative.com/a s/ZDI-18-3 https://ww oftware.com rt/security bulletins.ph	advisorie 79 vw.foxits m/suppo -	A-Fox- Foxit/18- 06-18/28
CV Scoring Scale (C	VSS)	3-	4 4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								
Injection: VSS- Cross Site Scripting								

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
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 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	https://zerodayiniti ative.com/advisorie s/ZDI-18-394 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/29
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 Shading objects. The issue results from the lack of proper validation of user- supplied data which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI- CAN-5393. CVE-ID:CVE-2018- 10474	https://zerodayiniti ative.com/advisorie s/ZDI-18-384 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/30
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	https://zerodayiniti ative.com/advisorie s/ZDI-18-350	A-Fox- Foxit/18- 06-18/31
			interaction is required to exploit	https://www.foxits	1

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

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

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions 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-5570. CVE-ID:CVE-2018-9966	oftware.com/suppo rt/security- bulletins.php	
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 Format actions 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-5571. CVE-ID:CVE-2018-9967	oftware.com/suppo rt/security- bulletins.php	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://zerodayiniti ative.com/advisorie s/ZDI-18-352 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/33

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			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. CVE-ID:CVE-2018-9968		
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 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	ative.com/advisorie s/ZDI-18-342	A-Fox- Foxit/18- 06-18/35

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			leverage this vulnerability to execute code under the context of the current process. Was ZDI- CAN-5620. CVE-ID:CVE-2018- 9958		
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 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. CVE-ID:CVE-2018-9965	oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/36
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 object. An attacker can leverage this vulnerability to execute code	oftware.com/suppo rt/security-	A-Fox- Foxit/18- 06-18/37

	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
CV Scoring Scale (CVSS)								
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								
Injection; XSS- Cross Site Scripting;								

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			under the context of the current process. Was ZDI-CAN-5618. CVE-ID:CVE-2018-9957		
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 setting the formatted Value attribute the process does not properly validate 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-5527. CVE-ID:CVE-2018- 9952	https://zerodayiniti ative.com/advisorie s/ZDI-18-336 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/38
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 setting the title attribute the process does not properly validate 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-5617.	oftware.com/suppo rt/security-	A-Fox- Foxit/18- 06-18/39

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									

Vulnerability Type(s)	Publish Date	CVSSS		Descrij	ption & CV	ID	Reference	e/Patch	NCIIPC ID
			CV	E-ID:CVE-2	2018-9956)			
Execute Code	17-05-2018	6.8			bility allow		https://zer	-	A-Fox-
			cod of 1	le on vuln Foxit Read	execute lerable ins ler 9.0.1.10	tallations)49. User	ative.com/a s/ZDI-18-3	38	Foxit/18- 06-18/40
			this targ	s vulneral get must vi	required t bility in isit a malici	that the ious page	https://ww oftware.cor rt/security- bulloting.pk	n/suppo -	
			spe hai	ecific flaw	malicious f exists wi of XFA Then settin	thin the Button	bulletins.pł	ιh	
			attı pro	ribute the operly valid	process of late the exi rior to pe	does not stence of			
			ope atta	erations o acker ca	on the ob	oject. An ge this			
			uno pro	der the con ocess. Wa	ntext of the	e current AN-5529.			
Execute Code	17-05-2018	6.8	atta cod	ackers to le on vuln	bility allow execute erable ins	arbitrary tallations	https://zer ative.com/a s/ZDI-18-3	advisorie	A-Fox- Foxit/18- 06-18/41
			inte this	of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page			https://ww oftware.cor rt/security	n/suppo	
			or spe	open a n ecific flaw	malicious exists wi nnotation'	file. The thin the	bulletins.pł		
			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-5435.						
CV Scoring Scale (CV	VSS)	3-4	^	ecess. Wa	5-6	6-7	7-8	8-9	9-10

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

 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-9962		
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 name attribute of OCG 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-5568. CVE-ID:CVE-2018-9964	https://zerodayiniti ative.com/advisorie s/ZDI-18-348 https://www.foxits oftware.com/suppo rt/security- bulletins.php	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://zerodayiniti ative.com/advisorie s/ZDI-18-343 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/43

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
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 rect 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-5434. CVE-ID:CVE-2018-9961	https://zerodayiniti ative.com/advisorie s/ZDI-18-345 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/44
Execute Code	17-05-2018	6.8	CVE-ID:CVE-2018-9961 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://zerodayiniti ative.com/advisorie s/ZDI-18-344 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/45
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	https://zerodayiniti ative.com/advisorie s/ZDI-18-353 https://www.foxits	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):
 CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the XFA boundItem method of 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-5579. CVE-ID:CVE-2018-9969	oftware.com/suppo rt/security- bulletins.php	
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 resolveNode method of 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-5531. CVE-ID:CVE-2018-9955	https://zerodayiniti ative.com/advisorie s/ZDI-18-339 https://www.foxits oftware.com/suppo rt/security- bulletins.php	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://zerodayiniti ative.com/advisorie s/ZDI-18-337 https://www.foxits oftware.com/suppo rt/security- bulletins.php	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): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								

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

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

6-7

4-5

3-4

7-8

8-9

9-10

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)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5401. CVE-ID:CVE-2018-10480		
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 typed arrays. The issue results from the lack of proper initialization of a pointer 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- 5380. CVE-ID:CVE-2018-9948	https://zerodayiniti ative.com/advisorie s/ZDI-18-332 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/53
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 U3D Texture Resource 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 data structure. An attacker can	oftware.com/suppo rt/security-	A-Fox- Foxit/18- 06-18/54

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10			
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL										
Injection; XSS- Cross Site Scripting;										

6-7

7-8

8-9

9-10

4-5

3-4

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5408. CVE-ID:CVE-2018-10481		
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 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 allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5490. CVE-ID:CVE-2018-1179	https://zerodayiniti ative.com/advisorie s/ZDI-18-317 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/55
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 PDF documents. 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-18-334 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/56

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10			
Vulnerability Type(s): CSRF-Cross Site Red	Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									

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	ative.com/advisorie s/ZDI-18-382 https://www.foxits oftware.com/suppo	A-Fox- Foxit/18- 06-18/58

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									

Injection; XSS- Cross Site Scripting;

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

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

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

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								

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-5419. CVE-ID:CVE-2018-10487		
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. 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. CVE-ID:CVE-2018-9978	https://zerodayiniti ative.com/advisorie s/ZDI-18-376 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/63
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. 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	https://zerodayiniti ative.com/advisorie s/ZDI-18-378 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/64

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attackercanleveragethisinconjunctionwithothervulnerabilitiesto executecodeinthecontextofthecurrentprocess.WasZDI-CAN-5430.CVE-ID:CVE-2018-9980		
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 Key Frame 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 data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5399. CVE-ID:CVE-2018-10479	https://zerodayiniti ative.com/advisorie s/ZDI-18-389 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/65
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 Light Node 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	oftware.com/suppo	A-Fox- Foxit/18- 06-18/66

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN- 5394. CVE-ID:CVE-2018-10475		
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 Model Node 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 structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN- 5395. CVE-ID:CVE-2018-10476	https://zerodayiniti ative.com/advisorie s/ZDI-18-386 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/67
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 Texture Coord Dimensions objects. 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	https://zerodayiniti 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 (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Red Injection; XSS- Cross Site Scripting;	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Den	ial of Service; I	NA- Not Applic	able; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5397. CVE-ID:CVE-2018-10478		
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 U3D Texture Image Format object. 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-5409. CVE-ID:CVE-2018-10482	https://zerodayiniti ative.com/advisorie s/ZDI-18-392 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/69
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 U3D Texture Height 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 data structure. An	https://www.foxits oftware.com/suppo	A-Fox- Foxit/18- 06-18/70

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL								

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5412. CVE-ID:CVE-2018-10485		
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. 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 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 arbitrary code in the context of the current process. Was ZDI- CAN-5755. CVE-ID:CVE-2018- 9972	https://zerodayiniti ative.com/advisorie s/ZDI-18-356 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/71
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. 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 ePub 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 buffer. An	https://zerodayiniti 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 (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attackercanleveragethisinconjunctionwithothervulnerabilitiestoexecutearbitrarycodeinthecontextarbitrarycodeinthecontextthecurrentprocess.WasZDI-CAN-5758.CVE-ID:CVE-2018-9973		
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. 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 JPEG2000 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. Was ZDI-CAN-5549. CVE-ID:CVE-2018-9963	https://zerodayiniti ative.com/advisorie s/ZDI-18-347 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/73
Execute Code Gain Information	17-05-2018	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. 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 U3D Final Maximum Resolution attribute. The issue results from the lack of proper validation of user- supplied data which can result in	https://zerodayiniti ative.com/advisorie s/ZDI-18-403 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/74

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL							
Injection; XSS- Cross Site Scripting;							

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-5426. CVE-ID:CVE-2018-10493			
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 BMP images. 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-5472. CVE-ID:CVE-2018- 9947	https://zerodayiniti ative.com/advisorie s/ZDI-18-331 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/75	
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 TIFF files. 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	https://zerodayiniti ative.com/advisorie s/ZDI-18-333 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/76	

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL							
Injection; XSS- Cross Site Scripting;							

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	, ,	A-Fox- Foxit/18- 06-18/78

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Rec Injection; XSS- Cross Site Scripting;	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Den	ial of Service; I	NA- Not Applic	able; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
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 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	ative.com/advisorie s/ZDI-18-404 https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Foxit/18- 06-18/79
PhantompdfRe	ader		10494		
Execute Code	24-05-2018	6.8	An issue was discovered in Foxia 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- 2018-7407	advisories/src- 2018-0018/ https://www.foxits oftware.com/suppo rt/security- bulletins.php	A-Fox- Phant/18 06-18/80
Execute Code	24-05-2018	6.8	An issue was discovered in Foxi Reader before 9.1 and	1 // /	A-Fox- Phant/18
				-	-

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code	24-05-2018	6.8	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 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 out-of-bounds write on a buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. CVE-ID:CVE-	2018-0017/ https://www.foxits oftware.com/suppo rt/security- bulletins.php https://srcincite.io/ advisories/src- 2018-0013/ https://www.foxits oftware.com/suppo rt/security- bulletins.php	06-18/81 A-Fox- Phant/18- 06-18/82
Execute Code	24-05-2018	6.8	2018-5675 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	https://srcincite.io/ advisories/src- 2018-0016/ https://www.foxits oftware.com/suppo rt/security-	A-Fox- Phant/18- 06-18/83

5-6

6-7

7-8

8-9

9-10

4-5

3-4

Vulnerability Type(s)	Publish Date	CVSSS		Descrip	otion & CV	ID	Reference	e/Patch	NCIIPC ID
			or spe pro pdf ima the use resu allo leve othe cod pro than 201	open a r cific flaw cessing o files wit ages. The lack of p r-supplied ult in a rea cated objection er vulneration e in the co cess a dif n CVE-201 .8-5679.	sit a malici nalicious exists wi f specially f specially h embed issue resures roper valid data wh d past the ect. An atta in conjunct abilities to ntext of th ferent vulues 18-5677 a CVE-ID:CV	file. The thin the v crafted ded u3d alts from dation of nich can end of an acker can tion with execute e current nerability nd CVE-	bulletins.pł	np	
Execute Code	24-05-2018	6.8	Th atta cod of 1 Pha inte this targ or spe pro pdf ima the use resu allo leve othe cod pro thai	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-2018-5677 and CVE- 2018-5680. CVE-ID:CVE-2018-		https://src advisories/ 2018-0015 https://ww oftware.con rt/security- bulletins.ph	/src- / /w.foxits n/suppo	A-Fox- Phant/18- 06-18/84	
Execute Code	24-05-2018	6.8			bility allow execute		https://src advisories/		A-Fox- Phant/18-
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	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-2018-5678	2018-0014/ 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	06-18/85 A-Fox- Phant/18- 06-18/86

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Rec	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Deni	ial of Service; N	NA- Not Applic	able; Sql-SQL
Injection: VSS- Cross Site Scripting:							

Injection; XSS- Cross Site Scripting;

ſ

Vulnerability Type(s)	Publish Date	CVSSS	Descri	ption & CV	ID	Referenc	e/Patch	NCIIPC ID
Execute Code Overflow Execute Code Overflow	24-05-2018	6.8	This vulnera attackers to code on vulr of Foxit Read PhantomPDF interaction is this vulnera target must v or open a b specific flaw processing of pdf files wir images. Craft file can trigg heap-based b can leverage execute code the current vulnerability 5674 and CV ID:CVE-2018 This vulnera attackers to code on vulr of Foxit Read PhantomPDF interaction is this vulnera target must v or open a b specific flaw processing of pdf files wir images. Craft file can trigg heap-based b can leverage execute code the current vulnerability 5676 and CV ID:CVE-2018	execute erable insider before before 9 required t bility in isit a malici malicious f exists wi of specially th embedo ted data in er an overfort ouffer. An this vulner under the of process a than C 7E-2018-56 -5676 bility allow execute herable insider before before 9 required t bility in isit a malici malicious f exists wi of specially th embedo ted data in er an overfort bility in isit a malici malicious f exists wi of specially th embedo ted data in er an overfort bility in isit a malici malicious f exists wi of specially th embedo ted data in er an overfort bility in isit a malici malicious f exists wi of specially th embedo ted data in er an overfort ouffer. An this vulner under the of process a than C 7E-2018-56	arbitrary tallations 9.1 and 1. User to exploit that the tous page file. The thin the rafted ded u3d the PDF flow of a attacker ability to context of different VE-2018- 78. CVE- 78. CVE- 78. CVE- 78. CVE- 78. CVE- 78. CVE- 79. and 9.1 and 9.1 and 9.1 and 9.1 and 9.1 user to exploit that the tous page file. The thin the rafted ded u3d the PDF flow of a attacker ability to context of different VE-2018- 78. CVE-	https://src advisories/ 2018-0011 https://ww oftware.con rt/security bulletins.pl https://src advisories/ 2018-0010 https://ww oftware.con rt/security bulletins.pl	/src- / ww.foxits m/suppo - hp incite.io/ /src- / ww.foxits m/suppo -	A-Fox- Phant/18- 06-18/87
		3-	4 4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Rec	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Den	ial of Service; I	NA- Not Applic	able; Sql-SQL
Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Desc	ription & CV	ID	Referenc	e/Patch	NCIIPC ID		
Hdfgroup										
Hdf5										
DoS	16-05-2018	4.3	H5Dbtree.c 1.10.2 libra remote den	on by ze _decode_key in the HE ury. It could tial of servic C-2018-1120	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	H5Dchunk.c 1.10.2 libra remote den	on by ze in H5D_chui : in the HI iry. It could ial of servic :-2018-1120	nk_init in DF HDF5 allow a ce attack.	Twi1ight/f				
DoS	16-05-2018	4.3	discovered H5O_chunk H5Ocache.c 1.10.2 libra remote den	inter derefer c_deserialize in the HE try. It could tial of servic C-2018-1120	in in DF HDF5 allow a ce attack.	Twi1ight/f	https://github.com/ Twi1ight/fuzzing- pocs/tree/master/h df5			
DoS	16-05-2018	5.8	discovered H5O_fill_nev H5O_fill_old in the HDF I could allow service or in	_decode in HDF5 1.10.2 7 a remote nformation 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			https://github.com/ Twi1ight/fuzzing- pocs/tree/master/h df5		A-Hdf- Hdf5/18- 06-18/93		
CV Scoring Scale (C	VSS)	3-4	4 4-5	5-6	6-7	7-8	8-9	9-10		
CV Scoring Scale (C Vulnerability Type	VSS) (s): CSRF-Cross Site									

Vulnerability Type(s)	Publish Date	CVSSS		Descrij	otion & CV	ID	Referenc	e/Patch	NCIIPC ID
IBM									
	tualize For ize V3700 Softw				reSpectrui twareStory		alize Softw 0 Software	vareStorw	ize V3500
CSRF	17-05-2018	6.8	Sto and 6.1 7.6 and cro cou exe una fro tru	rwize IBM l IBM Flas 6.2 6.3 6.4 7.6.1 7.7 l 8.1.1) ss-site req ald allow ecute authorized m 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 cker to and nsmitted website	https://exc orce.ibmclo vulnerabili 474	oud.com/	A-IBM- Spect/18- 06-18/94
DoS	17-05-2018	6.5	Sto and 6.1 7.6 aut sys acc or o X-F	rwize IBM l IBM Flas 6.2 6.3 6.4 7.6.1 7.7 l 8.1.1) henticated tem files th ess to incl causing a d orce ID		Virtualize roducts (3 7.4 7.5 7.8.1 8.1 low an access not have ting files vice. IBM	https://exc orce.ibmclo vulnerabili 363	oud.com/	A-IBM- Spect/18- 06-18/95
Gain Information	17-05-2018	3.5	IB Sto and 6.1 7.6 and privinte pos	1462https://exchangeIBM SAN Volume Controller IBMhttps://exchangeStorwize IBM Spectrum Virtualizeorce.ibmcloud.coand IBM FlashSystem products (vulnerabilities/16.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.53967.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1andand 8.1.1)could allow anauthenticated user to obtain theprivate key which could makeintercepting GUI communicationspossible. IBM X-Force ID CVE-ID:CVE-2018-1465				oud.com/	A-IBM- Spect/18- 06-18/96
Gain Information	17-05-2018	S		M SAN Vol rwize IBM I IBM Flas	ume Contro Spectrum V hSystem pr 4 7.1 7.2 7.	/irtualize roducts (https://exc orce.ibmclo vulnerabili 395	oud.com/	A-IBM- Spect/18- 06-18/97
CV Scoring Scale (CV	/SS)	3-4	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
			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 obtain sensitive information that they should not have authorization to read. IBM X-Force ID CVE- ID:CVE-2018-1464		
Gain Information	17-05-2018	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) web handler /DLSnap could allow an unauthenticated attacker to read arbitrary files on the system. IBM X-Force ID CVE- ID:CVE-2018-1438	https://exchange.xf orce.ibmcloud.com/ vulnerabilities/139 566	A-IBM- Spect/18- 06-18/98
Gain Information	17-05-2018	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) web handler /DownloadFile does not require authentication to read arbitrary files from the system. IBM X- Force ID CVE-ID:CVE-2018- 1433	https://exchange.xf orce.ibmcloud.com/ vulnerabilities/139 473	A-IBM- Spect/18- 06-18/99
NA	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) use weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X- Force ID CVE-ID:CVE-2018- 1466	https://exchange.xf orce.ibmcloud.com/ vulnerabilities/140 397	A-IBM- Spect/18- 06- 18/100
NA	17-05-2018	4	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (https://exchange.xf orce.ibmcloud.com/ vulnerabilities/140	A-IBM- Spect/18- 06-
CV Scoring Scale (CV	766)	3-4	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					L
Libjpeg					r
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		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	ChijinZ/security_ad	A-IJG- Libjp/18- 06-
CV Scoring Scale (C	VSS)	3-4	4 4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type	(s): CSRF-Cross Site s Site Scripting;	Request For	gery; Dir. TravDirectory Traversal; DoS-Dei	nial of Service; NA- Not Appli	cable; Sql-SQL

Vulnerability Type(s) Publish Date	CVSSS	Descri	ption & CV	ID	Reference	e/Patch	NCIIPC ID
		remote atta denial of sen fault) via a ID:CVE-2018	rvice (Segn crafted fi	nentation	r/libjpeg-v9	Ja	18/105
Ilias							
Ilias							
NA 17-05-2018	5.8	ILIAS 5.1.x 5 5.3.5 redirect a third-par return_to_url ID:CVE-2018	s a logged-i ty site paramete - 11119	in user to via the er. CVE-	https://ww e/docu/got rget=st_229 github.com eLearning/ mmit/01a2 dddf1da590 063797348	o.php?ta Phttps:// /ILIAS- ILIAS/co 4cf04fe8 ca49758 22b6	A-Ili- Ilias/18- 06- 18/106
XSS 17-05-2018	4.3	Services/COP PCSourceCod 5.2.x and 5.3 XSS. CVE-ID:	e.php in IL 8.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	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 II 3.x before ink attribu	LIAS 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 https:// /ILIAS- ILIAS/co 29858f2 1a6f8bf3	A-Ili- Ilias/18- 06- 18/108
XSS 17-05-2018	4.3	The RSS subsystem in ILIAS 5.1.x 5.2.x and 5.3.x before 5.3.5 has XSS via a URI to Services/Feeds/classes/class.ilEx ternalFeedItem.php. CVE-ID:CVE- 2018-11118			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 (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
				29f694acd0582bc6 26c7c8e62b519	
Imagemagick					
Imagemagick					
DoS	18-05-2018	4.3	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-25 there is a use-after-free in ReadOneMNGImage in coders/png.c which allows attackers to cause a denial of service via a crafted MNG image file that is mishandled in an MngInfoDiscardObject call. CVE- ID:CVE-2017-18272	1 // 8 //	A-Ima- Image/18 -06- 18/110
DoS Overflow	18-05-2018	4.3	In ImageMagick 7.0.7-23 Q16 x86_64 2018-01-24 there is a heap-based buffer over-read in ReadSUNImage in coders/sun.c 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	https://usn.ubuntu. com/3681- 1/https://github.co m/ImageMagick/Im ageMagick/issues/9 56https://lists.debi an.org/debian-lts- announce/2018/05 /msg00012.html	A-Ima- Image/18 -06- 18/111
NA	31-05-2018	6.8	In ImageMagick 7.0.7-36 Q16 theReadMATImage function in coders/mat.c allows attackers to cause a use after free via a crafted file. CVE-ID:CVE-2018-11624	1 // 8 //	A-Ima- Image/18 -06- 18/112
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 over- read via a crafted file. CVE- ID:CVE-2018-11625	https://usn.ubuntu. com/3681- 1/https://github.co m/ImageMagick/Im ageMagick/issues/1 156	A-Ima- Image/18 -06- 18/113
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	https://portal.msrc. microsoft.com/en- US/security- guidance/advisory/ CVE-2018-8176	A-Mic- Offic/18- 06- 18/114

5-6

6-7

7-8

8-9

9-10

4-5

3-4

Vulnerability Type(s)	Publish Date	CVSSS	Descr	iption & CV	ID	Reference	e/Patch	NCIIPC ID
			PowerPoint Execution affects Mic ID:CVE-201					
Podofo Project	:							
Podofo					-			
DoS	18-05-2018	4.3	An issue PoDoFo 0. PdfPage CVE 11255	9.5. The	vered in function . 8-	https://bug hat.com/sh gi?id=1575	ow_bug.c	A-Pod- Podof/18- 06- 18/115
DoS	18-05-2018	4.3		9.5. There Recursion	is an in the	https://bug hat.com/sh gi?id=1576	ow_bug.c	A-Pod- Podof/18- 06- 18/116
Wireshark								
Wireshark								
NA	22-05-2018	5	and 2.2.0 dissector co addressed epan/dissect avoiding dereference an SRV ro 2018-11356	uld crash. ' tors/packet- a NULL for an empty ecord. CVE	che DNS This was in dns.c by pointer name in -ID:CVE-	https://ww hark.org/se npa-sec-20 29.html https://bug ark.org/bug ow_bug.cgi 1 https://cod ark.org/rev web?p=wir t;a=commit 716ddba99 d033d9bc0 973	ecurity/w 18- gs.wiresh gzilla/sh ?id=1468 le.wiresh riew/git eshark.gi ;h=4425 374749b f4add2fb	A-Wir- Wires/18 -06- 18/117
NA	22-05-2018	5	and 2.2.0 dissector a	nd other d nsume is was addr c by ngths. CVE	the LTP issectors excessive ressed in rejecting	https://ww hark.org/se npa-sec-20 28.html https://bug ark.org/bug ow_bug.cgi 8	ecurity/w 18- gs.wiresh gzilla/sh	A-Wir- Wires/18 -06- 18/118
CV Scoring Scale (CV	VSS)	3-4	4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSSS		Descrij	otion & CV	ID	Referenc	e/Patch	NCIIPC ID
							https://coc ark.org/rev web?p=wir t;a=commit 33ef083b9 17747a83a faf6	view/git reshark.gi t;h=ab8a 732c891	
NA	22-05-2018	5	and diss add epa by a a n cert	2.2.0 to sector couressed n/dissecto avoiding a nalformed	x2.6.0 2.4.0 2.2.14 th ld crash. 7 ors/packet- use-after-f packet p nup. CVE	e Q.931 This was in q931.c Tree after	https://ww hark.org/se npa-sec-20 31.html https://ww n.org/secu 8/dsa-4212 https://cod ark.org/rev web?p=wir t;a=commit c3c8cec47f 0ced80644 52 https://list org/debian announce/ /msg00012 ps://bugs.v .org/bugzil bug.cgi?id=	ecurity/w 18- ww.debia rity/201 7 de.wiresh view/git reshark.gi t;h=ccb1a bbbf2e8 c005c652 cs.debian. i-lts- 2018/05 9.htmlhtt wireshark la/show_	A-Wir- Wires/18 -06- 18/119
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		
CV Scoring Scale (C	VSS)	3-	4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL
Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS		Descri	ption & CV	ID	Referenc	e/Patch	NCIIPC ID
							ark.org/rev web?p=win t;a=commi e91b14564 726bab099 1b	eshark.gi t;h=beaeb lfb9f86f0	
NA	22-05-2018	5	This epar ieee corr	s was n/dissecto 1905.c by rection to	rk2.6.0 th ector coul address ors/packet- y making o string 2018-1135	sed in a certain handling.	https://ww hark.org/s npa-sec-20 26.html https://bu ark.org/bu ow_bug.cgi 7 https://cod ark.org/rev web?p=win t;a=commi 7a4a43438 75ebb1066 251c	ecurity/w 18- gs.wiresh gzilla/sh ?id=1464 de.wiresh view/git reshark.gi t;h=cb51 87e74a2f	A-Wir- Wires/18 -06- 18/121
Overflow	22-05-2018	5	and DTA was epar gsm one over	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://bu ark.org/bu ow_bug.cgi 8https://co hark.org/r web?p=win t;a=commi 36c51f83a 24e8ee3a6 b24bhttps: ebian.org/s 2018/dsa- 4217https: wireshark. ity/wnpa-s 30.html	gzilla/sh ?id=1468 ode.wires eview/git reshark.gi t;h=a55b 7b96808 ce8429a //www.d security/ //www. org/secur	A-Wir- Wires/18 -06- 18/122
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 LDSS dissector could crash. This was addressed in epan/dissectors/packet-ldss.c by			https://wv hark.org/s npa-sec-20 25.html https://wv	A-Wir- Wires/18 -06- 18/123		
CV Scoring Scale (C	VSS)	3-	<u> </u>	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): CSRF-Cross Site Red Injection; XSS- Cross Site Scripting;	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Deni	ial of Service; I	NA- Not Applic	able; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV	ID	Reference/Pa	atch N	ICIIPC ID
Overflow	22-05-2018	5	In Wireshark2.6.0 th dissector could crash. T addressed epan/dissectors/packet- avoiding a buffer over packet status chunks ID:CVE-2018-11355	This was in rtcp.c by flow for s. CVE-	https://www.w hark.org/securi npa-sec-2018- 27.html https://bugs.wi ark.org/bugzilla ow_bug.cgi?id=1 3 https://code.wi ark.org/review, web?p=wiresha t;a=commit;h=9 7a5fd2c540f83 aca3b3647f5ccf 3	ity/w W -(1 iresh a/sh 1467 iresh /git ark.gi 99d2 7154	A-Wir- Vires/18 06- 8/125
			onOperating System (Ap	plication	0S)		
	anImagemagic nagemagickUbi		v				
DoS	18-05-2018	7.1	In ImageMagick 7.0.7-	-16 016	https://github.o	com/	A-Can-
			x86_64 2017-12-22 an loop vulnerability was the function ReadMIFFI coders/miff.c which attackers to cause a c service (CPU exhaustion crafted MIFF image fi ID:CVE-2017-18271	infinite found in mage in allows lenial of n) via a	ImageMagick/In Magick/issues/ https://lists.del org/debian-lts- announce/2018 /msg00012.htm https://usn.ubu com/3681-1/	mage D 1911 0 bian. 1 3/05 nl	ebia/18- 6- 8/126
DoS	18-05-2018	7.1	In ImageMagick 7.0.7- x86_64 2017-12-22 an loop vulnerability was the function ReadTXTH coders/txt.c which attackers to cause a co service (CPU exhaustion crafted image file mishandled in GetImageIndexInList ca ID:CVE-2017-18273	infinite found in mage in allows lenial of n) via a that is a	/ /		A-Can- ebia/18- 6- 8/127

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
	1		Operatingt System (OS)		
Microsoft					
Windows 10W Server 2016	indows 7Windo	ows 8.1W	indows Rt 8.1Windows Server 200	08Windows Server 20	12Windows
Overflow Memory Corruption	14-06-2018	7.6	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory aka "Media Foundation Memory Corruption Vulnerability." This affects Windows 7 Windows Server 2012 R2 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	microsoft.com/en- US/security- guidance/advisory/	O-Mic- Windo/18 -06- 18/128
	indows Server 2				1
NA	14-06-2018	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 10 Windows 10 Servers. CVE-ID:CVE-2018-8233	guidance/advisory/	O-Mic- Windo/18 -06- 18/129

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Red Injection; XSS- Cross Site Scripting;	quest Forgery;	Dir. TravDi	rectory Trave	rsal; DoS-Deni	ial of Service; I	NA- Not Applica	able; Sql-SQL