Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Apple					
Icloud;Itunes					
Gain Information	25-12-2017	4.3	An issue was discovered in certain Apple products. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. The issue involves the "APNs Server" component. It allows man-in-the-middle attackers to track users by leveraging mishandling of client certificates.**CVE ID : CVE-2017-13864**	https://support.apple.com/HT208328	A-APP-ICLOU-10118/1
Foxitsoftware					
Foxit Reader					
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. 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 yTsiz member of SIZ markers. 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-4977. **CVE ID : CVE-2017-16589**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/2
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/3

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. The specific flaw exists within the parsing of SOT markers. 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-4976. **CVE ID : CVE-2017-16588**		
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.2.25013. 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 util.printf. 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-5290. **CVE ID : CVE-2017-16584**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/4
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.2.25013. 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 ImageField node of XFA forms. 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	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/5

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5281. **CVE ID : CVE-2017-16580**		
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.2.25013. 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 vulnerability to execute code under the context of the current process. Was ZDI-CAN-5244. **CVE ID : CVE-2017-16579**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/6
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. 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 Image filters. 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-5079. **CVE ID : CVE-2017-16574**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/7
Execute Code	20-12-2017	4.3	This vulnerability allows remote	https://www.	A-FOX-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. 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 LZWDecode filters. 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-5078. **CVE ID : CVE-2017-16573**	foxitsoftware.com/support/security-bulletins.php	FOXIT-10118/8
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. 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 xOsiz member of SIZ markers. 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-5014. **CVE ID : CVE-2017-14822**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/9
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. User interaction is required to exploit this vulnerability in that the target must	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			visit a malicious page or open a malicious file. The specific flaw exists within the parsing of the xTsiz member of SIZ markers. 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-5013. **CVE ID : CVE-2017-14821**		
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. 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 tile index of the SOT marker in 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-5012. **CVE ID : CVE-2017-14820**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/11
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. 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 channel number member of the cdef box. The issue results from the lack of proper validation of user-	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/12

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-5011. **CVE ID : CVE-2017-14819**		
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive on vulnerable installations of Foxit Reader 8.3.1.21155. 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 embedded in PDF 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-4982. **CVE ID : CVE-2017-14818**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/13
Execute Code	20-12-2017	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.1.21155. 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 tile index member of SOT markers. 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	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/14

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZDI-CAN-4978. **CVE ID : CVE-2017-10956**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.2.25013. 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 removeField 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-5296. **CVE ID : CVE-2017-16587**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/15
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.2.25013. 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 addAnnot 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-5295. **CVE ID : CVE-2017-16586**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/16
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.2.25013. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/17

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific flaw exists within the app.response 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-5294. **CVE ID : CVE-2017-16585**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.2.25013. 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 datasets element of XFA forms. 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-5289. **CVE ID : CVE-2017-16583**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/18
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.2.25013. 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 clearItems XFA 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-5288.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/19

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 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2017-16582		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.2.25013. 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 author attribute of the Document object. 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-5282. **CVE ID : CVE-2017-16581**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/20
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.2.25013. 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 picture elements within XFA forms. 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-5216. **CVE ID : CVE-2017-16578**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/21
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/22

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific flaw exists within the alignment attribute of Field 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-5094. **CVE ID : CVE-2017-16577**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 XFA's field element. 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-5092. **CVE ID : CVE-2017-16576**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/23
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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's bind element. 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-5091. **CVE ID : CVE-2017-16575**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/24

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. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 FormCalc's closeDoc 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 to execute code in the context of the current process. Was ZDI-CAN-5073. **CVE ID : CVE-2017-16572**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/25
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 references to the app object from FormCalc. 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. Was ZDI-CAN-5072. **CVE ID : CVE-2017-16571**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/26
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 pageSpan	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/27

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			method of XFA Layout objects. 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. Was ZDI-CAN-5029. **CVE ID : CVE-2017-14837**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1. 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 modDate attribute of Annotation 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-5028. **CVE ID : CVE-2017-14836**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/28
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 page method of XFA Layout objects. 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. Was ZDI-CAN-5027. **CVE ID : CVE-2017-14835**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/29
Execute Code	20-12-2017	6.8	This vulnerability allows remote	https://www.	A-FOX-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 style attribute of FileAttachment annotation 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-5026. **CVE ID : CVE-2017-14834**	foxitsoftware.com/support/security-bulletins.php	FOXIT-10118/30
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 style attribute of Text Annotation 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-5025. **CVE ID : CVE-2017-14833**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/31
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 style	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/32

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attribute of Caret Annotation 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-5024. **CVE ID : CVE-2017-14832**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 author attribute of Circle Annotation 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-5023. **CVE ID : CVE-2017-14831**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/33
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 setFocus method of XFAScriptObject objects. 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. Was ZDI-CAN-5022.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/34

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2017-14830		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 openList method of XFAScriptObject objects. 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. Was ZDI-CAN-5021. **CVE ID : CVE-2017-14829**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/35
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 w method of XFA Layout objects. 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-5020. **CVE ID : CVE-2017-14828**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/36
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 append	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/37

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			method of XFA Node objects. 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-5019. **CVE ID : CVE-2017-14827**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 formNodes method of XFA Node objects. 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-5018. **CVE ID : CVE-2017-14826**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/38
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 remove method of XFAScriptObject objects. 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	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/39

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZDI-CAN-5017. **CVE ID : CVE-2017-14825**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 insert method of XFAScriptObject objects. 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-5016. **CVE ID : CVE-2017-14824**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/40
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 signer method of XFA's Signature objects. 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 in the context of the current process. Was ZDI-CAN-5015. **CVE ID : CVE-2017-14823**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/41
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. User interaction is required to exploit this vulnerability in	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/42

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the target must visit a malicious page or open a malicious file. The specific flaw exists within 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-4981. **CVE ID : CVE-2017-10959**		
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 value attribute of Field 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-4980. **CVE ID : CVE-2017-10958**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/43
Execute Code	20-12-2017	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.3.1.21155. 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 arrowEnd attribute of Annotation 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	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-10118/44

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			current process. Was ZDI-CAN-4979. **CVE ID : CVE-2017-10957**		
Graphicsmagick					
Graphicsmagick					
Overflow	20-12-2017	5.1	In GraphicsMagick 1.3.27a, there is a buffer over-read in ReadPALMImage in coders/palm.c when QuantumDepth is 8. **CVE ID : CVE-2017-17783**	https://sourceforge.net/p/graphicsmagick/bugs/529/	A-GRA-GRAPH-10118/45
Overflow	20-12-2017	6.8	In GraphicsMagick 1.3.27a, there is a heap-based buffer over-read in ReadOneJNGImage in coders/png.c, related to oFFs chunk allocation. **CVE ID : CVE-2017-17782**	https://sourceforge.net/p/graphicsmagick/bugs/530/	A-GRA-GRAPH-10118/46
Overflow	27-12-2017	6.8	In GraphicsMagick 1.4 snapshot-20171217 Q8, there is a heap-based buffer over-read in ReadMNGImage in coders/png.c, related to accessing one byte before testing whether a limit has been reached. **CVE ID : CVE-2017-17915**	http://hg.graphicsmagick.org/hg/GraphicsMagick/rev/1721f1b7e67a	A-GRA-GRAPH-10118/47
Overflow	27-12-2017	6.8	In GraphicsMagick 1.4 snapshot-20171217 Q8, there is a stack-based buffer over-read in WriteWEBPImage in coders/webp.c, related to an incompatibility with libwebp versions, 0.5.0 and later, that use a different structure type. **CVE ID : CVE-2017-17913**	http://hg.graphicsmagick.org/hg/GraphicsMagick/rev/6dda3c33f35f	A-GRA-GRAPH-10118/48
Overflow	27-12-2017	6.8	In GraphicsMagick 1.4 snapshot-20171217 Q8, there is a heap-based buffer over-read in ReadNewsProfile in coders/tiff.c, in which LocaleNCompare reads heap data beyond the allocated region. **CVE ID : CVE-2017-17912**	http://hg.graphicsmagick.org/hg/GraphicsMagick/rev/0d871e813a4f	A-GRA-GRAPH-10118/49
Imagemagick					
Imagemagick					
DoS	27-12-2017	4.3	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function GetImagePixelCache in magick/cache.c, which allows attackers	https://github.com/ImageMagick/ImageMagick/issues/	A-IMA-IMAGE-10118/50

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to cause a denial of service via a crafted MNG image file that is processed by ReadOneMNGImage. **CVE ID : CVE-2017-17887**	903	
DoS	27-12-2017	4.3	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service via a crafted psd image file. **CVE ID : CVE-2017-17886**	https://github.com/ImageMagick/ImageMagick/issues/874	A-IMA-IMAGE-10118/51
DoS	27-12-2017	4.3	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPICTImage in coders/pict.c, which allows attackers to cause a denial of service via a crafted PICT image file. **CVE ID : CVE-2017-17885**	https://github.com/ImageMagick/ImageMagick/issues/879	A-IMA-IMAGE-10118/52
DoS	27-12-2017	4.3	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function WriteOnePNGImage in coders/png.c, which allows attackers to cause a denial of service via a crafted PNG image file. **CVE ID : CVE-2017-17884**	https://github.com/ImageMagick/ImageMagick/issues/902	A-IMA-IMAGE-10118/53
DoS	27-12-2017	4.3	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPGXImage in coders/pgx.c, which allows attackers to cause a denial of service via a crafted PGX image file. **CVE ID : CVE-2017-17883**	https://github.com/ImageMagick/ImageMagick/issues/877	A-IMA-IMAGE-10118/54
DoS	27-12-2017	4.3	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted XPM image file. **CVE ID : CVE-2017-17882**	https://github.com/ImageMagick/ImageMagick/issues/880	A-IMA-IMAGE-10118/55
DoS	27-12-2017	4.3	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in	https://github.com/ImageM	A-IMA-IMAGE-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted MAT image file. **CVE ID : CVE-2017-17881**	agick/ImageMagick/issues/878	10118/56
NA	27-12-2017	5	ImageMagick 7.0.7-17 Q16 x86_64 has memory leaks in coders/msl.c, related to MSLPopImage and ProcessMSLScript, and associated with mishandling of MSLPushImage calls. **CVE ID : CVE-2017-17934**	https://github.com/ImageMagick/ImageMagick/issues/920	A-IMA-IMAGE-10118/57
Overflow	27-12-2017	6.8	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a stack-based buffer over-read in WriteWEBPImage in coders/webp.c, related to a WEBP_DECODER_ABI_VERSION check. **CVE ID : CVE-2017-17880**	https://github.com/ImageMagick/ImageMagick/issues/907	A-IMA-IMAGE-10118/58
Overflow	27-12-2017	6.8	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a heap-based buffer over-read in ReadOneMNGImage in coders/png.c, related to length calculation and caused by an off-by-one error. **CVE ID : CVE-2017-17879**	https://github.com/ImageMagick/ImageMagick/issues/906	A-IMA-IMAGE-10118/59
DoS	27-12-2017	7.1	In ImageMagick 7.0.7-16 Q16, a vulnerability was found in the function ReadOnePNGImage in coders/png.c, which allows attackers to cause a denial of service (ReadOneMNGImage large loop) via a crafted mng image file. **CVE ID : CVE-2017-17914**	https://github.com/ImageMagick/ImageMagick/issues/908	A-IMA-IMAGE-10118/60
Paid To Read Script Project					
Paid To Read Script					
Sql	18-12-2017	7.5	Paid To Read Script 2.0.5 has SQL Injection via the admin/userview.php uid parameter, the admin/viewemcamp.php fnum parameter, or the admin/viewvisitcamp.php fn parameter.**CVE ID : CVE-2017-17651**	NA	A-PAI-PAID - 10118/61
Sistemagpweb					

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 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Gpweb					
Execute Code Sql	18-12-2017	7.5	SQL injection vulnerability in Password Recovery in GPWeb 8.4.61 allows remote attackers to execute arbitrary SQL commands via the "checkemail" parameter.**CVE ID : CVE-2017-15875**	https://www.augustopereira.com.br/blog/seguranca-gpweb-8-4-61-multiplas-falhas-sqli-manipulacao-de-privilegios-uploads-sem-restricoes-exposicao-de-informacao-sensivel	A-SIS-GPWEB-10118/62
Application;Operating System (A/OS)					
Apple/Apple					
Apple Tv/Iphone Os					
NA	25-12-2017	5	An issue was discovered in certain Apple products. iOS before 11.2.1 is affected. tvOS before 11.2.1 is affected. The issue involves the "HomeKit" component. It allows remote attackers to modify the application state by leveraging incorrect message handling, as demonstrated by use of an Apple Watch to obtain an encryption key and unlock a door. **CVE ID : CVE-2017-13903**	https://support.apple.com/HT208359	A-APP-APPLE-10118/63
Apple Tv/Iphone Os;Mac Os X					
DoS Bypass	27-12-2017	5.6	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. The issue involves the "Kernel" component. It allows local users to bypass intended memory-read restrictions or cause a denial of service (system crash).	https://support.apple.com/HT208334	A-APP-APPLE-10118/64

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. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2017-7154		
Apple Tv/Iphone Os;Mac Os X;Watchos					
Bypass Obtained Information	25-12-2017	4.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2017-13869**	https://support.apple.com/HT208334	A-APP-APPLE-10118/65
Bypass Obtained Information	25-12-2017	4.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2017-13868**	https://support.apple.com/HT208334	A-APP-APPLE-10118/67
Bypass Obtained Information	25-12-2017	4.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2017-13865**	https://support.apple.com/HT208334	A-APP-APPLE-10118/68
Bypass	25-12-2017	4.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app that triggers type confusion. **CVE ID : CVE-2017-13855**	https://support.apple.com/HT208331	A-APP-APPLE-10118/69
DoS Execute	25-12-2017	9.3	An issue was discovered in certain	https://suppo	A-APP-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code Overflow memory corruption			Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13876**	rt.apple.com/ HT208334	APPLE-10118/70
DoS Execute Code Overflow memory corruption	25-12-2017	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13867**	https://support.apple.com/ HT208334	A-APP-APPLE-10118/71
DoS Execute Code Overflow memory corruption	25-12-2017	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13862**	https://support.apple.com/ HT208331	A-APP-APPLE-10118/72
DoS Execute Code Overflow memory corruption	27-12-2017	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "IOKit" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption)	https://support.apple.com/ HT208334	A-APP-APPLE-10118/73

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 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID		Patch	NCIIPC ID
			via a crafted app. **CVE ID : CVE-2017-7162**			
Apple Tv/Iphone Os;Watchos						
DoS Execute Code Overflow memory corruption	25-12-2017	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "IOSurface" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13861**		https://support.apple.com/HT208334	A-APP-APPLE-10118/74
Apple Tv;Icloud;Itunes;Safari/Iphone Os						
DoS Execute Code Overflow memory corruption	25-12-2017	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	**CVE ID : CVE-2017-13870**	https://support.apple.com/HT208334	A-APP-APPLE-10118/75
DoS Execute Code Overflow memory corruption	25-12-2017	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a		https://support.apple.com/HT208334	A-APP-APPLE-10118/76

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. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web site. **CVE ID : CVE-2017-13866**		
DoS Execute Code Overflow memory corruption	25-12-2017	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-13856**	https://support.apple.com/HT208334	A-APP-APPLE-10118/77
DoS Execute Code Overflow memory corruption	27-12-2017	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7160**	https://support.apple.com/HT208334	A-APP-APPLE-10118/78
DoS Execute Code Overflow memory corruption	27-12-2017	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7157**	https://support.apple.com/HT208328	A-APP-APPLE-10118/79

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 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
DoS Execute Code Overflow memory corruption	27-12-2017	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7156**	https://support.apple.com/HT208328	A-APP-APPLE-10118/80
OPERATING SYSTEM(OS)					
Apple					
Iphone Os					
NA	27-12-2017	4.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. The issue involves the "Mail Message Framework" component. It allows remote attackers to spoof the address bar via a crafted web site. **CVE ID : CVE-2017-7152**	https://support.apple.com/HT208334	O-APP-IPHON-10118/81
Bypass	25-12-2017	5	An issue was discovered in certain Apple products. iOS before 11.2 is affected. The issue involves the "Mail" component. It might allow remote attackers to bypass an intended encryption protection mechanism by leveraging incorrect S/MIME certificate selection. **CVE ID : CVE-2017-13874**	https://support.apple.com/HT208334	O-APP-IPHON-10118/82
DoS Execute Code Overflow memory corruption	25-12-2017	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. The issue involves the "IOMobileFrameBuffer" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13879**	https://support.apple.com/HT208334	O-APP-IPHON-10118/83

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 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Iphone Os;Mac Os X					
Gain Information	25-12-2017	4.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. The issue involves the "Mail Drafts" component. It allows man-in-the-middle attackers to read e-mail content by leveraging mishandling of S/MIME credential encryption. **CVE ID : CVE-2017-13860**	https://support.apple.com/HT208331	O-APP-IPHON-10118/84
DoS Execute Code Overflow memory corruption	25-12-2017	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. The issue involves the "IOKit" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13847**	https://support.apple.com/HT208334	O-APP-IPHON-10118/85
Mac Os X					
NA	25-12-2017	5	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "Mail" component. It allows remote attackers to read cleartext e-mail content (for which S/MIME encryption was intended) by leveraging the lack of installation of an S/MIME certificate by the recipient. **CVE ID : CVE-2017-13871**	https://support.apple.com/HT208331	O-APP-MAC O-10118/86
DoS Bypass	25-12-2017	5.6	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "Intel Graphics Driver" component. It allows local users to bypass intended memory-read restrictions or cause a denial of service (out-of-bounds read and system crash). **CVE ID : CVE-2017-13878**	https://support.apple.com/HT208331	O-APP-MAC O-10118/87
Overflow	27-12-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.13.2	https://support.apple.com/	O-APP-MAC O-

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 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is affected. The issue involves the "Screen Sharing Server" component. It allows attackers to obtain root privileges for reading files by leveraging screen-sharing access. **CVE ID : CVE-2017-7158**	HT208331	10118/88
DoS Execute Code Overflow memory corruption	25-12-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13883**	https://support.apple.com/HT208331	O-APP-MAC O-10118/89
DoS Execute Code	25-12-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (out-of-bounds read) via a crafted app. **CVE ID : CVE-2017-13875**	https://support.apple.com/HT208331	O-APP-MAC O-10118/90
Execute Code	25-12-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "IOKit" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2017-13858**	https://support.apple.com/HT208331	O-APP-MAC O-10118/91
Execute Code	25-12-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "IOKit" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2017-13848**	https://support.apple.com/HT208331	O-APP-MAC O-10118/92
DoS Execute Code Overflow memory corruption	27-12-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a	https://support.apple.com/HT208331	O-APP-MAC O-10118/94

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 Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7163**		
DoS Execute Code Overflow memory corruption	27-12-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "IOAcceleratorFamily" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7159**	https://support.apple.com/HT208331	O-APP-MAC O-10118/95
DoS Execute Code Overflow memory corruption	27-12-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7155**	https://support.apple.com/HT208331	O-APP-MAC O-10118/96