National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale : 3-10 **01-15 Dec 2017** **Vol. 04 No.21**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Adobe					
Acrobat;Acrobat Dc;Acrobat Reader;Acrobat Reader Dc					
NA	09-12-2017	4.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The issue is a stack exhaustion problem within the JavaScript API, where the computation does not correctly control the amount of recursion that can happen with respect to system resources. **CVE ID : CVE-2017-16419**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/1
Bypass restriction	09-12-2017	4.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a Same Origin Policy security bypass vulnerability, affecting files on the local system, etc. **CVE ID : CVE-2017-16369**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/2
Bypass	09-12-2017	4.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a security bypass vulnerability when handling XFDF files. **CVE ID : CVE-2017-16361**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/3
Bypass	09-12-2017	5	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098	https://helpx.adobe.co	A-ADO-ACROB-

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
			and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a security bypass vulnerability in the AcroPDF plugin. **CVE ID : CVE-2017-16366**	m/security /products/ acrobat/ap sb17-36.html	161217/4
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is in the part of the JavaScript engine that handles annotation abstraction. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16420**	https://helpx.adobe.com/security /products/ acrobat/ap sb17-36.html	A-ADO-ACROB-161217/5
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of the image conversion module that handles XPS files. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16418**	https://helpx.adobe.com/security /products/ acrobat/ap sb17-36.html	A-ADO-ACROB-161217/6
NA	09-12-2017	9.3	An issue was discovered in Adobe	https://hel	A-ADO-

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
			Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of the font parsing module. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16417**	px.adobe.com/security/products/acrobat/apsb17-36.html	ACROB-161217/7
Execute Code	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a computation that writes data past the end of the intended buffer; the computation is part of the image conversion module that handles Enhanced Metafile Format Plus (EMF+) data. The vulnerability is a result of an out of range pointer offset that is used to access sub-elements of an internal data structure. An attacker can potentially leverage the vulnerability to corrupt sensitive data or execute arbitrary code. **CVE ID : CVE-2017-16416**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/8
Execute Code	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a computation that writes data past the end of the intended	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/9

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer; the computation is a part of the functionality that handles font encodings. The vulnerability is a result of out of range pointer offset that is used to access sub-elements of an internal data structure. An attacker can potentially leverage the vulnerability to corrupt sensitive data or execute arbitrary code. **CVE ID : CVE-2017-16415**		
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of the JavaScript API module responsible for form field computation. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16414**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/10
Execute Code	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a computation that writes data past the end of the intended buffer; the computation is part of the XPS to PDF conversion module, when processing TIFF files. The vulnerability is a result of an out of range pointer offset that is used to access sub-elements of an internal data structure. An attacker can potentially leverage the	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/11

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

Vulnerability Type(s): CSRF-Cross Site 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
			vulnerability to corrupt sensitive data or execute arbitrary code. **CVE ID : CVE-2017-16413**		
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs because of a computation that reads data that is past the end of the target buffer; the computation is part of the XPS conversion module, when handling a JPEG resource. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16412**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/12
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of the WebCapture module, related to an internal hash table implementation. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16411**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/13
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355	https://helpx.adobe.com/security/products/	A-ADO-ACROB-161217/14

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier versions, and 11.0.22 and earlier versions. The vulnerability is a result of untrusted input that is used to calculate an array index; the calculation occurs in the image conversion module, when processing GIF files. The vulnerability leads to an operation that can write to a memory location that is outside of the memory addresses allocated for the data structure. The specific scenario leads to a write access to a memory location that does not belong to the relevant process address space. **CVE ID : CVE-2017-16410**	acrobat/apsb17-36.html	
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of the Adobe graphics module responsible for displaying textual data. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16409**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/15
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of the WebCapture module. The use of an invalid (out-of-range) pointer offset	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/16

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16408**		
Execute Code	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a computation that writes data past the end of the intended buffer; the computation is part of handling an EMF EMR_BITBLT record. The vulnerability is a result of an out of range pointer offset that is used to access sub-elements of an internal data structure. An attacker can potentially leverage the vulnerability to corrupt sensitive data or execute arbitrary code. **CVE ID : CVE-2017-16407**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/17
Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a type confusion vulnerability in the EMF processing module. The issue causes the program to access an object using an incompatible type, leading to an out of bounds memory access. Attackers can exploit the vulnerability by using the out of bounds access for unintended reads, writes, or frees -- potentially leading to code corruption, control-flow hijack, or information leak attack. **CVE ID : CVE-2017-16406**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/18
NA	09-12-2017	9.3	An issue was discovered in Adobe	https://hel	A-ADO-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of Acrobat's page display functionality. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16405**	px.adobe.com/security/products/acrobat/apsb17-36.html	ACROB-161217/19
Execute Code	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a computation that writes data past the end of the intended buffer; the computation is part of processing Enhanced Metafile Format Plus (EMF+). The vulnerability is a result of an out of range pointer offset that is used to access sub-elements of an internal data structure. An attacker can potentially leverage the vulnerability to corrupt sensitive data or execute arbitrary code. **CVE ID : CVE-2017-16404**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/20
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/21

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the image conversion module that processes Enhanced Metafile Format Plus (EMF+) data. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16403**		
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of the JPEG 2000 module. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16402**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/22
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of an image conversion, specifically in Enhanced Metafile Format Plus (EMF +) processing modules. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/23

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-2017-16401		
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of the JPEG 2000 parser. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16400**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/24
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This issue is due to an untrusted pointer dereference in the XPS parsing module. In this scenario, the input is crafted in a way that the computation results in pointers to memory locations that do not belong to the relevant process address space. The dereferencing operation is a read operation, and an attack can result in sensitive data exposure. **CVE ID : CVE-2017-16399**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/25
Execute Code Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the JavaScript engine. The mismatch	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/26

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. 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
			between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-16398**		
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of Enhanced Metafile Format (EMF) processing within the image conversion module. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16397**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/27
Execute Code Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer access with an incorrect length value in the TIFF processing module. Crafted input causes a mismatch between allocated buffer size and the access allowed by the computation. If an attacker can adequately control the accessible memory then this vulnerability can be leveraged to achieve arbitrary code execution. **CVE ID : CVE-2017-16396**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/28

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 Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer access with an incorrect length value in the image conversion module when processing Enhanced Metafile Format (EMF). Crafted EMF input (EMR_STRETCHDIBITS) causes a mismatch between allocated buffer size and the access allowed by the computation. If an attacker can adequately control the accessible memory then this vulnerability can be leveraged to achieve arbitrary code execution. **CVE ID : CVE-2017-16395**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/29
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of the Web Capture module. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16394**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/30
Execute Code Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a use after free vulnerability	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/31

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the JavaScript engine. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-16393**		
Execute Code Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer access with an incorrect length value in the JPEG processing module. Crafted input with an unexpected JPEG file segment size causes a mismatch between allocated buffer size and the access allowed by the computation. If an attacker can adequately control the accessible memory then this vulnerability can be leveraged to achieve arbitrary code execution. **CVE ID : CVE-2017-16392**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/32
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is a result of untrusted input that is used to calculate an array index; the calculation occurs in the printing functionality. The vulnerability leads to an operation that can write to a memory location that is outside of the memory addresses allocated for the data structure. The specific scenario leads to a write access to a memory location that does not belong to the relevant process address	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/33

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. 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
			space. **CVE ID : CVE-2017-16391**		
Execute Code Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the JavaScript engine API. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-16390**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/34
Execute Code	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the JavaScript engine. The mismatch between an old and a new object can provide an attacker with unintended memory access. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-16389**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/35
Execute Code Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the JavaScript API engine. The mismatch between an old and a new object can provide an attacker with unintended memory access --	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/36

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
			potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-16388**		
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of the JPEG2000 codec. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16387**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/37
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of the XPS2PDF conversion engine. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16386**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/38
Execute Code Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355	https://helpx.adobe.com/security/products/	A-ADO-ACROB-161217/39

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. 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
			and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer access with an incorrect length value in TIFF parsing during XPS conversion. Crafted TIFF image input causes a mismatch between allocated buffer size and the access allowed by the computation. If an attacker can adequately control the accessible memory then this vulnerability can be leveraged to achieve arbitrary code execution. **CVE ID : CVE-2017-16385**	acrobat/apsb17-36.html	
Overflow Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer over-read in the exif processing module for a PNG file (during XPS conversion). Invalid input leads to a computation where pointer arithmetic results in a location outside valid memory locations belonging to the buffer. An attack can be used to obtain sensitive information, such as object heap addresses, etc. **CVE ID : CVE-2017-16384**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/40
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a heap overflow vulnerability when processing a JPEG file embedded within an XPS document. **CVE ID : CVE-2017-16383**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/41
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098	https://helpx.adobe.co	A-ADO-ACROB-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of the image conversion module. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16382**	m/security/products/acrobat/apsb17-36.html	161217/42
Execute Code Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer access with an incorrect length value when processing TIFF files embedded within an XPS document. Crafted TIFF image input causes a mismatch between allocated buffer size and the access allowed by the computation. If an attacker can adequately control the accessible memory then this vulnerability can be leveraged to achieve arbitrary code execution. **CVE ID : CVE-2017-16381**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/43
Bypass	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a security bypass vulnerability for a certain file-type extension. Acrobat maintains both a blacklist and whitelist (the user can specify an allowed attachment).	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/44

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			However, any file extensions that are neither on the blacklist nor the whitelist can still be opened after displaying a warning prompt. **CVE ID : CVE-2017-16380**		
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a type confusion overflow vulnerability in the graphics rendering engine. **CVE ID : CVE-2017-16379**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/45
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is due to a computation that accesses a pointer that has not been initialized; the computation occurs during internal AST thread manipulation. In this case, a computation defines a read from an unexpected memory location. Therefore, an attacker might be able to read sensitive portions of memory. **CVE ID : CVE-2017-16378**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/46
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is due to a computation that accesses a pointer that has not been initialized in the main DLL. In this case, a computation defines a read from an unexpected memory location. Therefore, an attacker might be able to	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/47

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
			read sensitive portions of memory. **CVE ID : CVE-2017-16377**		
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is a part of the MakeAccessible plugin. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16376**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/48
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This issue is due to an untrusted pointer dereference in the JavaSscript API engine. In this scenario, the JavaScript input is crafted in way that the computation results in pointers to memory locations that do not belong to the relevant process address space. The dereferencing operation is a read operation, and an attack can result in sensitive data exposure. **CVE ID : CVE-2017-16375**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/49
Overflow Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer over-read in the	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/50

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. 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
			JPEG 2000 module. An invalid JPEG 2000 input code stream leads to a computation where the pointer arithmetic results in a location outside valid memory locations belonging to the buffer. An attack can be used to obtain sensitive information, such as object heap addresses, etc. **CVE ID : CVE-2017-16374**		
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This issue is due to an untrusted pointer dereference. In this scenario, the input is crafted in way that the computation results in pointers to memory locations that do not belong to the relevant process address space. The dereferencing operation is a read operation, and an attack can result in sensitive data exposure. **CVE ID : CVE-2017-16373**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/51
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This issue is due to untrusted pointer dereference in the JavaScript API engine. In this scenario, the JavaScript input is crafted in way that the computation results with pointer to memory locations that do not belong to the relevant process address space. The dereferencing operation is a read operation, and an attack can result with sensitive data exposure. **CVE ID : CVE-2017-16372**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/52
Overflow	09-12-2017	9.3	An issue was discovered in Adobe	https://hel	A-ADO-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This issue is due to an untrusted pointer dereference in the JavaScript engine. In this scenario, the input is crafted in a way that the computation results in pointers to memory locations that do not belong to the relevant process address space. The dereferencing operation is a read operation, and an attack can result in sensitive data exposure. **CVE ID : CVE-2017-16371**	px.adobe.com/security/products/acrobat/apsb17-36.html	ACROB-161217/53
NA	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability occurs because of a computation that reads data that is past the end of the target buffer; the computation is a part of the JavaScript engine. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure. **CVE ID : CVE-2017-16370**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/54
Execute Code Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability leads to a stack-based buffer overflow condition in the internal Unicode string manipulation module. It is triggered by an invalid PDF file, where a crafted Unicode string causes an out of bounds	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/55

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
			memory access of a stack allocated buffer, due to improper checks when manipulating an offset of a pointer to the buffer. Attackers can exploit the vulnerability and achieve arbitrary code execution if they can effectively control the accessible memory. **CVE ID : CVE-2017-16368**		
Overflow Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a type confusion overflow vulnerability. The vulnerability leads to an out of bounds memory access. Attackers can exploit the vulnerability by using the out of bounds access for unintended reads or writes -- potentially leading to code corruption, control-flow hijack, or an information leak attack. **CVE ID : CVE-2017-16367**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/56
Overflow Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer over-read in the True Type2 Font parsing module. A corrupted cmap table input leads to a computation where the pointer arithmetic results in a location outside valid memory locations belonging to the buffer. An attack can be used to obtain sensitive information, such as object heap addresses, etc. **CVE ID : CVE-2017-16365**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/57
Overflow	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098	https://helpx.adobe.co	A-ADO-ACROB-

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
			and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This issue is due to an untrusted pointer dereference when handling number format dictionary entries. In this scenario, the input is crafted in way that the computation results in pointers to memory locations that do not belong to the relevant process address space. The dereferencing operation is a read operation, and an attack can result in sensitive data exposure. **CVE ID : CVE-2017-16364**	m/security/products/acrobat/apsb17-36.html	161217/58
Overflow Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. The vulnerability is caused by a buffer over-read in the module that handles character codes for certain textual representations. Invalid input leads to a computation where the pointer arithmetic results in a location outside valid memory locations belonging to the buffer. An attack can be used to obtain sensitive information, such as object heap addresses, etc. **CVE ID : CVE-2017-16363**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/59
Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of an out of bounds read vulnerability in the MakeAccesible plugin, when handling font data. It causes an out of bounds memory	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/60

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. 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
			access, which sometimes triggers an access violation exception. Attackers can exploit the vulnerability by using the out of bounds access for unintended reads, writes, or frees, potentially leading to code corruption, control-flow hijack, or an information leak attack. **CVE ID : CVE-2017-16362**		
Execute Code Memory corruption Obtain Information	09-12-2017	9.3	An issue was discovered in Adobe Acrobat and Reader: 2017.012.20098 and earlier versions, 2017.011.30066 and earlier versions, 2015.006.30355 and earlier versions, and 11.0.22 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the MakeAccessible plugin, when creating an internal data structure. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-16360**	https://helpx.adobe.com/security/products/acrobat/apsb17-36.html	A-ADO-ACROB-161217/61
Coldfusion					
XSS	01-12-2017	4.3	Adobe ColdFusion has a cross-site scripting (XSS) vulnerability. This affects Update 4 and earlier versions for ColdFusion 2016, and Update 12 and earlier versions for ColdFusion 11. **CVE ID : CVE-2017-11285**	https://helpx.adobe.com/security/products/coldfusion/apsb17-30.html	A-ADO-COLDF-161217/62
NA	01-12-2017	5	Adobe ColdFusion has an XML external entity (XXE) injection vulnerability. This affects Update 4 and earlier versions for ColdFusion 2016, and Update 12 and earlier versions for ColdFusion 11. **CVE ID : CVE-2017-11286**	https://helpx.adobe.com/security/products/coldfusion/apsb17-30.html	A-ADO-COLDF-161217/63
NA	01-12-2017	7.5	Adobe ColdFusion has an Untrusted	https://hel	A-ADO-

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
			Data Deserialization vulnerability. This affects Update 4 and earlier versions for ColdFusion 2016, and Update 12 and earlier versions for ColdFusion 11. **CVE ID : CVE-2017-11284**	px.adobe.com/security/products/coldfusion/apsb17-30.html	COLDF-161217/64
NA	01-12-2017	7.5	Adobe ColdFusion has an Untrusted Data Deserialization vulnerability. This affects Update 4 and earlier versions for ColdFusion 2016, and Update 12 and earlier versions for ColdFusion 11. **CVE ID : CVE-2017-11283**	https://helpx.adobe.com/security/products/coldfusion/apsb17-30.html	A-ADO-COLDF-161217/65
Connect					
NA	09-12-2017	4.3	An issue was discovered in Adobe Connect 9.6.2 and earlier versions. A UI Redress (or Clickjacking) vulnerability exists. This issue has been resolved by adding a feature that enables Connect administrators to protect users from UI redressing (or clickjacking) attacks. **CVE ID : CVE-2017-11290**	https://helpx.adobe.com/security/products/connect/apsb17-35.html	A-ADO-CONNE-161217/66
XSS	09-12-2017	4.3	An issue was discovered in Adobe Connect 9.6.2 and earlier versions. A reflected cross-site scripting vulnerability exists that can result in information disclosure. **CVE ID : CVE-2017-11289**	https://helpx.adobe.com/security/products/connect/apsb17-35.html	A-ADO-CONNE-161217/67
XSS	09-12-2017	4.3	An issue was discovered in Adobe Connect 9.6.2 and earlier versions. A reflected cross-site scripting vulnerability exists that can result in information disclosure. **CVE ID : CVE-2017-11288**	https://helpx.adobe.com/security/products/connect/apsb17-35.html	A-ADO-CONNE-161217/68
XSS	09-12-2017	4.3	An issue was discovered in Adobe Connect 9.6.2 and earlier versions. A reflected cross-site scripting vulnerability exists that can result in information disclosure.	https://helpx.adobe.com/security/products/connect/ap	A-ADO-CONNE-161217/69

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-2017-11287	sb17-35.html	
Bypass	09-12-2017	6.4	An issue was discovered in Adobe Connect 9.6.2 and earlier versions. A Server-Side Request Forgery (SSRF) vulnerability exists that could be abused to bypass network access controls. **CVE ID : CVE-2017-11291**	https://helpx.adobe.com/security/products/connect/apsb17-35.html	A-ADO-CONNE-161217/70
Digital Editions					
Gain Information	09-12-2017	4.3	An issue was discovered in Adobe Digital Editions 4.5.6 and earlier versions. Adobe Digital Editions parses crafted XML files in an unsafe manner, which could lead to sensitive information disclosure. **CVE ID : CVE-2017-11273**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-39.html	A-ADO-DIGIT-161217/71
Memory corruption Obtain Information	09-12-2017	5	An issue was discovered in Adobe Digital Editions 4.5.6 and earlier versions. An exploitable memory corruption vulnerability exists, which could lead to disclosure of memory addresses. **CVE ID : CVE-2017-11301**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-39.html	A-ADO-DIGIT-161217/72
Memory corruption Obtain Information	09-12-2017	5	An issue was discovered in Adobe Digital Editions 4.5.6 and earlier versions. An exploitable memory corruption vulnerability exists, which could lead to disclosure of memory addresses. **CVE ID : CVE-2017-11300**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-39.html	A-ADO-DIGIT-161217/73
Memory corruption Obtain Information	09-12-2017	5	An issue was discovered in Adobe Digital Editions 4.5.6 and earlier versions. An exploitable memory corruption vulnerability exists, which could lead to disclosure of memory addresses. **CVE ID : CVE-2017-11299**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-	A-ADO-DIGIT-161217/74

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. 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
				39.html	
Memory corruption Obtain Information	09-12-2017	5	An issue was discovered in Adobe Digital Editions 4.5.6 and earlier versions. An exploitable memory corruption vulnerability exists, which could lead to disclosure of memory addresses. **CVE ID : CVE-2017-11298**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-39.html	A-ADO-DIGIT-161217/75
Memory corruption Obtain Information	09-12-2017	5	An issue was discovered in Adobe Digital Editions 4.5.6 and earlier versions. An exploitable memory corruption vulnerability exists, which could lead to disclosure of memory addresses. **CVE ID : CVE-2017-11297**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-39.html	A-ADO-DIGIT-161217/76
Experience Manager					
XSS	09-12-2017	4.3	An issue was discovered in Adobe Experience Manager 6.3, 6.2, 6.1, 6.0. A cross-site scripting vulnerability in Apache Sling Servlets Post 2.3.20 has been resolved in Adobe Experience Manager. **CVE ID : CVE-2017-11296**	https://helpx.adobe.com/security/products/experience-manager/apsb17-41.html	A-ADO-EXPER-161217/77
XSS	09-12-2017	4.3	An issue was discovered in Adobe Experience Manager 6.3, 6.2, 6.1, 6.0. Adobe Experience Manager has a reflected cross-site scripting vulnerability in the HtmlRendererServlet. **CVE ID : CVE-2017-3109**	https://helpx.adobe.com/security/products/experience-manager/apsb17-41.html	A-ADO-EXPER-161217/78
Gain Information	09-12-2017	5	An issue was discovered in Adobe Experience Manager 6.3, 6.2, 6.1, 6.0. Sensitive tokens are included in http GET requests under certain circumstances. **CVE ID : CVE-2017-3111**	https://helpx.adobe.com/security/products/experience-manager/apsb17-	A-ADO-EXPER-161217/79

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				41.html	
Photoshop					
Execute Code	09-12-2017	7.5	An issue was discovered in Adobe Photoshop 18.1.1 (2017.1.1) and earlier versions. An exploitable use-after-free vulnerability exists. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-11304**	https://helpx.adobe.com/security/products/photoshop/apsb17-34.html	A-ADO-PHOTO-161217/80
Execute Code Overflow Memory corruption	09-12-2017	7.5	An issue was discovered in Adobe Photoshop 18.1.1 (2017.1.1) and earlier versions. An exploitable memory corruption vulnerability exists. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2017-11303**	https://helpx.adobe.com/security/products/photoshop/apsb17-34.html	A-ADO-PHOTO-161217/81
Robohelp					
XSS	01-12-2017	4.3	Adobe RoboHelp has a cross-site scripting (XSS) vulnerability. This affects versions before RH12.0.4.460 and RH2017 before RH2017.0.2. **CVE ID : CVE-2017-3104**	https://helpx.adobe.com/security/products/robohelp/apsb17-25.html	A-ADO-ROBOH-161217/82
NA	01-12-2017	5.8	Adobe RoboHelp has an Open Redirect vulnerability. This affects versions before RH12.0.4.460 and RH2017 before RH2017.0.2. **CVE ID : CVE-2017-3105**	https://helpx.adobe.com/security/products/robohelp/apsb17-25.html	A-ADO-ROBOH-161217/83
Ark-web					
A-member					
Execute Code Sql	01-12-2017	7.5	SQL injection vulnerability in the A-Member and A-Member for MT cloud versions 3.8.6 and earlier allows an attacker to execute arbitrary SQL commands via unspecified vectors. **CVE ID : CVE-2017-10898**	https://jvn.jp/en/jp/JVN78501037/index.html	A-ARK-A-MEM-161217/84
A-reserve					

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 Sql	01-12-2017	7.5	SQL injection vulnerability in the A-Reserve and A-Reserve for MT cloud versions 3.8.6 and earlier allows an attacker to execute arbitrary SQL commands via unspecified vectors. **CVE ID : CVE-2017-10899**	https://jvn.jp/en/jp/JVN78501037/index.html	A-ARK-A-RES-161217/85
Fiyo					
Fiyo Cms					
Sql	04-12-2017	5	Fiyo CMS 2.0.7 has SQL injection in /system/site.php via $_REQUEST['link']. **CVE ID : CVE-2017-17102**	https://github.com/FiyoCMS/FiyoCMS/issues/9	A-FIY-FIYO -161217/86
Sql	04-12-2017	6.5	Fiyo CMS 2.0.7 has SQL injection in /apps/app_user/sys_user.php via $_POST[name] or $_POST[email]. This vulnerability can lead to escalation from normal user privileges to administrator privileges. **CVE ID : CVE-2017-17103**	https://github.com/FiyoCMS/FiyoCMS/issues/10	A-FIY-FIYO -161217/87
Gain Information	04-12-2017	7.8	Fiyo CMS 2.0.7 has an arbitrary file read vulnerability in dapur/apps/app_theme/libs/check_file.php via $_GET['src'] or $_GET['name']. **CVE ID : CVE-2017-17104**	https://github.com/FiyoCMS/FiyoCMS/issues/11	A-FIY-FIYO -161217/88
Geovap					
Reliance-scada					
XSS	04-12-2017	4.3	A Cross-site Scripting issue was discovered in Geovap Reliance SCADA Version 4.7.3 Update 2 and prior. This vulnerability could allow an unauthenticated attacker to inject arbitrary code. **CVE ID : CVE-2017-16721**	NA	A-GEO-RELIA-161217/89
GNU					
Binutils					
DoS	04-12-2017	4.3	The coff_slurp_reloc_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1,	NA	A-GNU-BINUT-161217/90

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
			allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted COFF based file. **CVE ID : CVE-2017-17123**		
DoS Overflow	04-12-2017	6.8	The load_debug_section function in readelf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via an ELF file that lacks section headers. **CVE ID : CVE-2017-17126**	NA	A-GNU-BINUT-161217/91
DoS Overflow	04-12-2017	6.8	nm.c and objdump.c in GNU Binutils 2.29.1 mishandle certain global symbols, which allows remote attackers to cause a denial of service (_bfd_elf_get_symbol_version_string buffer over-read and application crash) or possibly have unspecified other impact via a crafted ELF file. **CVE ID : CVE-2017-17125**	NA	A-GNU-BINUT-161217/92
DoS Overflow	04-12-2017	6.8	The _bfd_coff_read_string_table function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not properly validate the size of the external string table, which allows remote attackers to cause a denial of service (excessive memory consumption, or heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted COFF binary. **CVE ID : CVE-2017-17124**	NA	A-GNU-BINUT-161217/93
DoS Overflow	04-12-2017	6.8	The dump_relocs_in_section function in objdump.c in GNU Binutils 2.29.1 does not check for reloc count integer overflows, which allows remote attackers to cause a denial of service (excessive memory allocation, or heap-	NA	A-GNU-BINUT-161217/94

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
			based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PE file. **CVE ID : CVE-2017-17122**		
DoS Overflow	04-12-2017	6.8	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (memory access violation) or possibly have unspecified other impact via a COFF binary in which a relocation refers to a location after the end of the to-be-relocated section. **CVE ID : CVE-2017-17121**	NA	A-GNU-BINUT-161217/95
Glibc					
Overflow	05-12-2017	6.8	The malloc function in the GNU C Library (aka glibc or libc6) 2.26 could return a memory block that is too small if an attempt is made to allocate an object whose size is close to SIZE_MAX, potentially leading to a subsequent heap overflow. This occurs because the per-thread cache (aka tcache) feature enables a code path that lacks an integer overflow check. **CVE ID : CVE-2017-17426**	https://sourceware.org/bugzilla/show_bug.cgi?id=22375	A-GNU-GLIBC-161217/96
IBM					
Sterling File Gateway					
Gain Information	07-12-2017	4	IBM Sterling File Gateway 2.2 could allow an authenticated attacker to obtain sensitive information such as login ids on the system. IBM X-Force ID: 128626. **CVE ID : CVE-2017-1487**	http://www.ibm.com/support/docview.wss?uid=swg22010552	A-IBM-STERL-161217/97
Gain Information	07-12-2017	4.3	IBM Sterling File Gateway 2.2 could allow an unauthorized user to view files they should not have access to providing they know the directory location of the file. IBM X-Force ID: 128695. **CVE ID : CVE-2017-1497**	http://www.ibm.com/support/docview.wss?uid=swg22010738	A-IBM-STERL-161217/98
Websphere Mq					

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
NA	07-12-2017	4	IBM WebSphere MQ 7.5, 8.0, and 9.0 could allow an authenticated user to insert messages with a corrupt RFH header into the channel which would cause it to restart. IBM X-Force ID: 127803. **CVE ID : CVE-2017-1433**	http://www.ibm.com/support/docview.wss?uid=swg22005525	A-IBM-WEBSP-161217/99
Inedo					
Otter					
DoS	01-12-2017	7.5	Indeo Otter through 1.7.4 mishandles a "</script>" substring in an initial DP payload, which allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact, as demonstrated by the Plan Editor. **CVE ID : CVE-2017-17086**	https://inedo.myjetbrains.com/youtrack/issue/ILIB-11	A-INE-OTTER-161217/100
Libav					
Libav					
DoS Overflow	04-12-2017	4.3	The h264_slice_init function in libavcodec/h264_slice.c in Libav 12.2 allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted file. **CVE ID : CVE-2017-17128**	https://bugzilla.libav.org/show_bug.cgi?id=1104	A-LIB-LIBAV-161217/101
DoS	04-12-2017	4.3	The vc1_decode_frame function in libavcodec/vc1dec.c in Libav 12.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file. **CVE ID : CVE-2017-17127**	https://bugzilla.libav.org/show_bug.cgi?id=1099	A-LIB-LIBAV-161217/102
DoS Overflow	04-12-2017	6.8	The ff_free_picture_tables function in libavcodec/mpegpicture.c in Libav 12.2 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file, related to vc1_decode_i_blocks_adv. **CVE ID : CVE-2017-17130**	https://bugzilla.libav.org/show_bug.cgi?id=1100	A-LIB-LIBAV-161217/103
DoS	04-12-2017	6.8	The ff_vc1_mc_4mv_chroma4 function in libavcodec/vc1_mc.c in Libav 12.2 allows remote attackers to cause a	https://bugzilla.libav.org/show_b	A-LIB-LIBAV-161217/

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
			denial of service (segmentation fault and application crash) or possibly have unspecified other impact via a crafted file. **CVE ID : CVE-2017-17129**	ug.cgi?id=1101	104
Libtiff					
Libtiff					
DoS Overflow	02-12-2017	6.8	tools/pal2rgb.c in pal2rgb in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (TIFFSetupStrips heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted TIFF file. **CVE ID : CVE-2017-17095**	NA	A-LIB-LIBTI-161217/105
Sdnsproxy Project					
Sdnsproxy					
DoS	01-12-2017	5	sDNSProxy.exe ver1.1.0.0 and earlier allows remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2017-10895**	https://jvn.jp/en/jp/JVN71291160/index.html	A-SDN-SDNSP-161217/106
Sony					
Media Go					
Gain privileges	01-12-2017	9.3	Untrusted search path vulnerability in Media Go version 3.2.0.191 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2017-10891**	https://jvn.jp/en/jp/JVN08517069/index.html	A-SON-MEDIA-161217/107
Music Center					
Gain privileges	01-12-2017	9.3	Untrusted search path vulnerability in Music Center for PC version 1.0.00 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2017-10892**	https://jvn.jp/en/jp/JVN08517069/index.html	A-SON-MUSIC-161217/108
Streamrelay					
Streamrelay					
DoS	01-12-2017	5	StreamRelay.NET.exe ver2.14.0.7 and earlier allows remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2017-10894**	https://jvn.jp/en/jp/JVN71291160/index.html	A-STR-STREA-161217/109

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
Tgsoft					
Vir.it Explorer					
DoS Gain privileges	08-12-2017	4.6	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to gain privileges or cause a denial of service (Arbitrary Write) via a \\.\Viragtlt DeviceIoControl request of 0x82730020, a different vulnerability than CVE ID : CVE-2017-17050. **CVE ID : CVE-2017-17468**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82730020	A-TGS-VIR.I-161217/110
DoS Gain privileges	08-12-2017	4.6	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to gain privileges or cause a denial of service (Arbitrary Write) via a \\.\Viragtlt DeviceIoControl request of 0x82730088. **CVE ID : CVE-2017-17466**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82730088	A-TGS-VIR.I-161217/111
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82736068. **CVE ID : CVE-2017-17475**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82736068	A-TGS-VIR.I-161217/112
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82730070. **CVE ID : CVE-2017-17474**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82730070	A-TGS-VIR.I-161217/113
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82730050. **CVE ID : CVE-2017-17473**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82	A-TGS-VIR.I-161217/114

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
				730050	
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82730030. **CVE ID : CVE-2017-17472**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82730030	A-TGS-VIR.I-161217/115
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82732140. **CVE ID : CVE-2017-17471**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82732140	A-TGS-VIR.I-161217/116
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82730054. **CVE ID : CVE-2017-17470**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82730054	A-TGS-VIR.I-161217/117
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82730008, a different vulnerability than CVE ID : CVE-2017-16948. **CVE ID : CVE-2017-17469**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82730008	A-TGS-VIR.I-161217/118
DoS Overflow	08-12-2017	6.1	TG Soft Vir.IT eXplorer Lite 8.5.42 allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact via a \\.\Viragtlt DeviceIoControl request of 0x82730074. **CVE ID : CVE-2017-17467**	https://github.com/rubyfly/Vir.IT-explorer_POC/tree/master/0x82730074	A-TGS-VIR.I-161217/119

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
Wordpress					
Wordpress					
XSS	02-12-2017	3.5	wp-includes/functions.php in WordPress before 4.9.1 does not require the unfiltered_html capability for upload of .js files, which might allow remote attackers to conduct XSS attacks via a crafted file. **CVE ID : CVE-2017-17092**	NA	A-WOR-WORDP-161217/120
Bypass	02-12-2017	6.5	wp-admin/user-new.php in WordPress before 4.9.1 sets the newbloguser key to a string that can be directly derived from the user ID, which allows remote attackers to bypass intended access restrictions by entering this string. **CVE ID : CVE-2017-17091**	NA	A-WOR-WORDP-161217/121
XSS	02-12-2017	3.5	wp-includes/feed.php in WordPress before 4.9.1 does not properly restrict enclosures in RSS and Atom fields, which might allow attackers to conduct XSS attacks via a crafted URL. **CVE ID : CVE-2017-17094**	NA	A-WOR-WORDP-161217/122
XSS	02-12-2017	3.5	wp-includes/general-template.php in WordPress before 4.9.1 does not properly restrict the lang attribute of an HTML element, which might allow attackers to conduct XSS attacks via the language setting of a site. **CVE ID : CVE-2017-17093**	NA	A-WOR-WORDP-161217/123
Application;Operating System (A/OS)					
Adobe/Redhat					
Flash Player/Enterprise Linux Desktop;Enterprise Linux Server;Enterprise Linux Workstation					
Execute Code Overflow Memory corruption	01-12-2017	7.5	Adobe Flash Player has an exploitable memory corruption vulnerability in the MP4 atom parser. Successful exploitation could lead to arbitrary code execution. This affects 26.0.0.151 and earlier. **CVE ID : CVE-2017-11282**	https://helpx.adobe.com/security/products/flash-player/apsb17-28.html	A-ADO-FLASH-161217/124
Exec Code	01-12-2017	7.5	Adobe Flash Player has an exploitable	https://hel	A-ADO-

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
Overflow Memory corruption			memory corruption vulnerability in the text handling function. Successful exploitation could lead to arbitrary code execution. This affects 26.0.0.151 and earlier. **CVE ID : CVE-2017-11281**	px.adobe.com/security/products/flash-player/apsb17-28.html	FLASH-161217/125
OPERATING SYSTEM(OS)					
Google					
Android					
Overflow	05-12-2017	4.4	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a race condition in a multimedia driver can potentially lead to a buffer overwrite. **CVE ID : CVE-2017-9718**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/126
NA	05-12-2017	4.4	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in the camera driver, the function "msm_ois_power_down" is called without a mutex and a race condition can occur in variable "*reg_ptr" of sub function "msm_camera_config_single_vreg". **CVE ID : CVE-2017-9708**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/127
NA	05-12-2017	4.4	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a race condition in a Camera driver can lead to a Use After Free condition. **CVE ID : CVE-2017-9703**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/128
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing the QCA_NL80211_VENDOR_SUBCMD_SET_TXPOWER_SCALE vendor command, in which attribute QCA_WLAN_VENDOR_ATTR_TXPOWER	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/129

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

Vulnerability Type(s): CSRF-Cross Site 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
			_SCALE contains fewer than 1 byte, a buffer overrun occurs. **CVE ID : CVE-2017-14901**		
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing the QCA_NL80211_VENDOR_SUBCMD_GET_CHAIN_RSSI vendor command, in which attribute QCA_WLAN_VENDOR_ATTR_MAC_ADDR contains fewer than 6 bytes, a buffer overrun occurs. **CVE ID : CVE-2017-14900**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/130
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing the QCA_NL80211_VENDOR_SUBCMD_SET_TXPOWER_SCALE_DECR_DB vendor command, in which attribute QCA_WLAN_VENDOR_ATTR_TXPOWER_SCALE_DECR_DB contains fewer than 1 byte, a buffer overrun occurs. **CVE ID : CVE-2017-14899**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/131
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing the QCA_NL80211_VENDOR_SUBCMD_SET_TXPOWER_SCALE vendor command, in which attribute QCA_WLAN_VENDOR_ATTR_TXPOWER_SCALE contains fewer than 1 byte, a buffer overrun occurs. **CVE ID : CVE-2017-14898**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/132
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, there is a memory allocation without a length field validation in the	https://source.android.com/security/bulletin/pixel/01-	O-GOO-ANDRO-161217/133

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mobicore driver which can result in an undersize buffer allocation. Ultimately this can result in a kernel memory overwrite.**CVE ID : CVE-2017-14896**	12-2017	
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, when updating custom EDID (hdmi_tx_sysfs_wta_edid), if edid_size, which is controlled by userspace, is too large, a buffer overflow occurs. **CVE ID : CVE-2017-9722**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/134
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, IOCTL interface to send QMI NOTIFY REQ messages can be called from multiple contexts which can result in buffer overflow of msg cache. **CVE ID : CVE-2017-9710**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/135
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, buffer overwrite is possible in fw_name_store if image name is 64 characters. **CVE ID : CVE-2017-9700**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/136
Overflow	05-12-2017	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improperly specified offset/size values for a submission command could cause a math operation to overflow and could result in an access to arbitrary memory. The combined pointer will overflow and possibly pass further checks intended to avoid accessing unintended memory. **CVE ID : CVE-2017-9698**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/137
NA	06-12-2017	4.6	An elevation of privilege vulnerability in the Broadcom wireless driver. Product: Android. Versions: Android	https://source.android.com/secur	O-GOO-ANDRO-161217/

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
			kernel. Android ID A-63930471. References: BC-V2017092501. **CVE ID : CVE-2017-13161**	ity/bulletin /pixel/01-12-2017	138
Overflow	05-12-2017	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing a specially crafted cfg80211 vendor command, a buffer over-read can occur. **CVE ID : CVE-2017-14905**	https://source.android.com/security/bulletin /pixel/01-12-2017	O-GOO-ANDRO-161217/ 139
Overflow	05-12-2017	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing the SENDACTIONFRAME IOCTL, a buffer over-read can occur if the payload length is less than 7. **CVE ID : CVE-2017-14903**	https://source.android.com/security/bulletin /pixel/01-12-2017	O-GOO-ANDRO-161217/ 140
Gain Information	06-12-2017	5	An information disclosure vulnerability in the Android media framework (libmedia drm). Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-62872384. **CVE ID : CVE-2017-13152**	https://source.android.com/security/bulletin /pixel/01-12-2017	O-GOO-ANDRO-161217/ 141
Gain Information	06-12-2017	5	An information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-65025028. **CVE ID : CVE-2017-0879**	https://source.android.com/security/bulletin /pixel/01-12-2017	O-GOO-ANDRO-161217/ 142
NA	05-12-2017	6.9	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, due to a race condition in the GLink kernel driver, a Use After Free condition can potentially occur. **CVE ID : CVE-2017-14902**	https://source.android.com/security/bulletin /01-12-2017	O-GOO-ANDRO-161217/ 143
DoS	06-12-2017	7.1	A denial of service vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-	https://source.android.com/security/bulletin	O-GOO-ANDRO-161217/ 144

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
			65717533. **CVE ID : CVE-2017-13148**	/01-12-2017	
DoS	06-12-2017	7.1	A denial of service vulnerability in the Android media framework (libskia). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID A-65646012. **CVE ID : CVE-2017-0880**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/145
NA	05-12-2017	7.2	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a crafted binder request can cause an arbitrary unmap in MediaServer. **CVE ID : CVE-2017-14904**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/146
Overflow	05-12-2017	7.2	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while handling the QSEOS_RPMB_CHECK_PROV_STATUS_COMMAND, a userspace buffer is directly accessed in kernel space. **CVE ID : CVE-2017-14897**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/147
NA	05-12-2017	7.2	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, after a subsystem reset, iwpriv is not giving correct information. **CVE ID : CVE-2017-14895**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/148
Overflow	05-12-2017	7.2	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, there is a possibility of stack corruption due to buffer overflow of Partition name while converting ascii string to unicode string in function HandleMetaImgFlash. **CVE ID : CVE-2017-11007**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/149
NA	06-12-2017	7.2	An elevation of privilege vulnerability in the Android system (art). Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0,	https://source.android.com/secur	O-GOO-ANDRO-161217/

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
			7.1.1, 7.1.2, 8.0. Android ID A-64211847. **CVE ID : CVE-2017-13156**	ity/bulletin/01-12-2017	150
NA	06-12-2017	7.2	An elevation of privilege vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-63666573. **CVE ID : CVE-2017-13154**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/151
NA	06-12-2017	7.2	An elevation of privilege vulnerability in the Android media framework (libaudioservice). Product: Android. Versions: 8.0. Android ID A-65280854. **CVE ID : CVE-2017-13153**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/152
Overflow	05-12-2017	7.5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a buffer overflow can occur while reading firmware logs. **CVE ID : CVE-2017-15813**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/153
NA	05-12-2017	7.5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a privilege escalation vulnerability exists in telephony. **CVE ID : CVE-2017-9709**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/154
Gain Information	06-12-2017	7.8	An information disclosure vulnerability in the Android system (activitymanagerservice). Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-32879772. **CVE ID : CVE-2017-13159**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/155
Gain Information	06-12-2017	7.8	An information disclosure vulnerability in the Android system (activitymanagerservice). Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-32879915. **CVE ID : CVE-2017-13158**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/156
Gain Information	06-12-2017	7.8	An information disclosure vulnerability in the Android system	https://source.android	O-GOO-ANDRO-

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
			(activitymanagerservice). Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-32990341. **CVE ID : CVE-2017-13157**	.com/security/bulletin/01-12-2017	161217/157
Overflow	05-12-2017	9.3	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in a WiFI driver function, an integer overflow leading to heap buffer overflow may potentially occur. **CVE ID : CVE-2017-11043**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/158
Execute Code	06-12-2017	9.3	A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-63874456. **CVE ID : CVE-2017-13151**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/159
NA	05-12-2017	10	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, cryptographic strength is reduced while deriving disk encryption key. **CVE ID : CVE-2017-14907**	https://source.android.com/security/bulletin/pixel/01-12-2017	O-GOO-ANDRO-161217/160
NA	05-12-2017	10	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a Use After Free condition can occur during positioning. **CVE ID : CVE-2017-11006**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/161
NA	05-12-2017	10	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a Use After Free condition can occur during a deinitialization path. **CVE ID : CVE-2017-11005**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/162
Exec Code	06-12-2017	10	A remote code execution vulnerability in the Android system (bluetooth). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID A-37160362. **CVE ID : CVE-2017-13160**	https://source.android.com/security/bulletin/01-12-2017	O-GOO-ANDRO-161217/163

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
Ismartalarm					
Cubeone Firmware					
Execute Code Gain Information	01-12-2017	5	Password file exposure in firmware in iSmartAlarm CubeOne version 2.2.4.8 and earlier allows attackers to execute arbitrary commands with administrative privileges by retrieving credentials from this file. **CVE ID : CVE-2017-13664**	https://poppopretn.com/2017/11/30/public-disclosure-firmware-vulnerabilities-in-ismartalarm-cubeone/	O-ISM-CUBEO-161217/164
Ntt-east					
Pwr-q200 Firmware					
NA	01-12-2017	5	PWR-Q200 does not use random values for source ports of DNS query packets, which allows remote attackers to conduct DNS cache poisoning attacks. **CVE ID : CVE-2017-10874**	http://web116.jp/shop/hikari_p/q200/q200_00.html	O-NTT-PWR-Q-161217/165
Princeton					
Ptw-wms1 Firmware					
Overflow	01-12-2017	5	Buffer overflow in PTW-WMS1 firmware version 2.000.012 allows remote attackers to conduct denial-of-service attacks via unspecified vectors. **CVE ID : CVE-2017-10901**	https://jvn.jp/en/jp/JVN98295787/index.html	O-PRI-PTW-W-161217/166
Bypass	01-12-2017	7.5	PTW-WMS1 firmware version 2.000.012 allows remote attackers to bypass access restrictions to obtain or delete data on the disk via unspecified vectors. **CVE ID : CVE-2017-10900**	https://jvn.jp/en/jp/JVN98295787/index.html	O-PRI-PTW-W-161217/167
NA	01-12-2017	10	Improper authentication issue in PTW-WMS1 firmware version 2.000.012 allows remote attackers to log in to the device with root privileges and conduct arbitrary operations via unspecified vectors. **CVE ID : CVE-2017-10903**	https://jvn.jp/en/jp/JVN98295787/index.html	O-PRI-PTW-W-161217/168
Execute Code	01-12-2017	10	PTW-WMS1 firmware version	https://jvn.	O-PRI-

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
			2.000.012 allows remote attackers to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2017-10902**	jp/en/jp/JVN98295787/index.html	PTW-W-161217/169
Operating System; Application (OS/A)					
Canonical;Debian/X					
Ubuntu Linux/Debian Linux/Libxcursor					
Overflow	01-12-2017	5	libXcursor before 1.1.15 has various integer overflows that could lead to heap buffer overflows when processing malicious cursors, e.g., with programs like GIMP.**CVE ID : CVE-2017-16612**	https://bugzilla.suse.com/show_bug.cgi?id=1065386	O-CAN-UBUNT-161217/170
Debian/Wireshark					
Debian Linux/Wireshark					
NA	01-12-2017	5	In Wireshark 2.4.0 to 2.4.2 and 2.2.0 to 2.2.10, the CIP Safety dissector could crash. This was addressed in epan/dissectors/packet-cipsafety.c by validating the packet length. **CVE ID : CVE-2017-17085**	https://www.wireshark.org/security/wnpa-sec-2017-49.html	O-DEB-DEBIA-161217/171
NA	01-12-2017	5	In Wireshark 2.4.0 to 2.4.2 and 2.2.0 to 2.2.10, the IWARP_MPA dissector could crash. This was addressed in epan/dissectors/packet-iwarp-mpa.c by validating a ULPDU length. **CVE ID : CVE-2017-17084**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14236	O-DEB-DEBIA-161217/172
A	01-12-2017	5	In Wireshark 2.4.0 to 2.4.2 and 2.2.0 to 2.2.10, the NetBIOS dissector could crash. This was addressed in epan/dissectors/packet-netbios.c by ensuring that write operations are bounded by the beginning of a buffer. **CVE ID : CVE-2017-17083**	https://www.wireshark.org/security/wnpa-sec-2017-48.html	O-DEB-DEBIA-161217/173

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;