National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale:0-10 01 Dec - 15 Dec 2018 Vol. 05 No. 23

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Google					
Chrome					
Overflow	2018-12-11	6.8	An integer overflow leading to a heap buffer overflow in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2018-18341**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/1
N/A	2018-12-11	4.3	Incorrect handling of alert box display in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to present confusing browser UI via a crafted HTML page. **CVE ID : CVE-2018-18346**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/2
Overflow	2018-12-11	6.8	Heap buffer overflow in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-	A-GOO-CHRO-201218/3

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-18335	desktop.html	
Overflow	2018-12-11	6.8	Incorrect object lifecycle in MediaRecorder in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2018-18340**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/4
Overflow	2018-12-11	6.8	Incorrect object lifecycle in WebAudio in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2018-18339**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/5
N/A	2018-12-11	6.8	Incorrect handing of paths leading to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2018-18343**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/6
N/A	2018-12-04	4.3	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform	https://chromereleases.googleblog.com/2018/04/stabl	A-GOO-CHRO-201218/7

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2018-6107**	e-channel-update-for-desktop.html	
N/A	2018-12-04	4.3	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2018-6098**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/8
Overflow	2018-12-04	6.8	Inline metadata in GarbageCollection in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2018-6094**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/9
+Info	2018-12-04	4.3	A lack of CORS checks in Blink in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page. **CVE ID : CVE-2018-6099**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/10
N/A	2018-12-04	4.3	Missing confusable characters in Internationalization in	https://chromerelease	A-GOO-CHRO-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Google Chrome prior to 66.0.3359.106 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. **CVE ID : CVE-2018-6102**	s.googleblog.com/2018/04/stable-channel-update-for-desktop.html	201218/11
Bypass	2018-12-04	4.3	A stagnant permission prompt in Prompts in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to bypass permission policy via a crafted HTML page. **CVE ID : CVE-2018-6103**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/12
Exec Code Overflow	2018-12-04	6.8	An integer overflow on 32-bit systems in WebAssembly in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. **CVE ID : CVE-2018-6092**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/13
Exec Code Overflow	2018-12-04	6.8	An integer overflow that lead to a heap buffer-overflow in Skia in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.ht	A-GOO-CHRO-201218/14

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-6090	ml	
N/A	2018-12-11	6.8	Incorrect handling of failed navigations with invalid URLs in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to trick a user into executing javascript in an arbitrary origin via a crafted HTML page. **CVE ID : CVE-2018-18347**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/15
Exec Code	2018-12-04	6.8	A use-after-free in WebAssembly in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. **CVE ID : CVE-2018-6087**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/16
Exec Code	2018-12-04	6.8	A double-eviction in the Incognito mode cache that lead to a user-after-free in Networking Disk Cache in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code via a crafted HTML page. **CVE ID : CVE-2018-6086**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/17
+Info	2018-12-04	4.3	Inappropriate dismissal of file picker on keyboard events in Blink in Google Chrome prior	https://chromereleases.googleblo	A-GOO-CHRO-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 66.0.3359.106 allowed a remote attacker to read local files via a crafted HTML page. **CVE ID : CVE-2018-6095**	g.com/2018/04/stable-channel-update-for-desktop.html	201218/18
N/A	2018-12-04	4.3	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2018-6105**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/19
N/A	2018-12-04	4.3	A lack of CORS checks, after a Service Worker redirected to a cross-origin PDF, in Service Worker in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page. **CVE ID : CVE-2018-6089**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/20
N/A	2018-12-11	6.8	Incorrect handling of Reflect.construct in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. **CVE ID : CVE-2018-18359**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/21

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow	2018-12-11	6.8	Incorrect, thread-unsafe use of SkImage in Canvas in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2018-18338**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/22
N/A	2018-12-11	6.8	Incorrect handling of stylesheets leading to a use after free in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2018-18337**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/23
N/A	2018-12-11	6.8	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2018-18336**	https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/24
Exec Code	2018-12-04	6.8	An iterator-invalidation bug in PDFium in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-	A-GOO-CHRO-201218/25

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-6088	desktop.html	
N/A	2018-12-04	4.3	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2018-6104**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/26
Exec Code	2018-12-04	6.8	Re-entry of a destructor in Networking Disk Cache in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code via a crafted HTML page. **CVE ID : CVE-2018-6085**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/27
N/A	2018-12-04	4.3	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted HTML page. **CVE ID : CVE-2018-6108**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/28
N/A	2018-12-11	6.8	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to	https://chromereleases.googleblog.com/201	A-GOO-CHRO-201218/29

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2018-17481**	8/12/stable-channel-update-for-desktop.html	
N/A	2018-12-04	4.3	A nullptr dereference in WebAssembly in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. **CVE ID : CVE-2018-6116**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/30
Bypass	2018-12-04	4.3	Inappropriate setting of the SEE_MASK_FLAG_NO_UI flag in file downloads in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to potentially bypass OS malware checks via a crafted HTML page. **CVE ID : CVE-2018-6115**	https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-201218/31
IBM					
Marketing Platform					
N/A	2018-12-07	5.5	IBM Marketing Platform 9.1.0, 9.1.2, and 10.1 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or	http://www.ibm.com/support/docview.wss?uid=ibm10744217	A-IBM-MARK-201218/32

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			consume memory resources. IBM X-Force ID: 139029. **CVE ID : CVE-2018-1424**		
N/A	2018-12-07	5.5	IBM Marketing Platform 9.1.0, 9.1.2 and 10.1 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 152855. **CVE ID : CVE-2018-1920**	http://www.ibm.com/support/docview.wss?uid=ibm10744217	A-IBM-MARK-201218/33
Qradar Security Information And Event Manager					
N/A	2018-12-05	5.5	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 147709. **CVE ID : CVE-2018-1730**	https://www.ibm.com/support/docview.wss?uid=ibm10742741&myns=swgother&mynp=OCSSBQAC&mync=E&cm_sp=swgother-_-OCSSBQAC-_-E	A-IBM-QRAD-201218/34
Kubernetes					
Kubernetes					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2018-12-05	7.5	In all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade requests in the kube-apiserver allowed specially crafted requests to establish a connection through the Kubernetes API server to backend servers, then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection. **CVE ID : CVE-2018-1002105**	https://groups.google.com/forum/#!topic/kubernetes-announce/GVllWCg6L88, https://github.com/kubernetes/kubernetes/issues/71411	A-KUB-KUBE-201218/35
Metinfo					
Metinfo					
XSS	2018-12-03	4.3	Metinfo 6.1.3 has reflected XSS via the admin/column/move.php lang_columnerr4 parameter. **CVE ID : CVE-2018-19835**	N/A	A-MET-METI-201218/36
Zohocorp					
Manageengine Opmanager					
XSS	2018-12-06	4.3	Zoho ManageEngine OpManager 12.3 before 123237 has XSS in the domain controller.	N/A	A-ZOH-MANA-201218/37

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-19921		
OS					
Microsoft					
Windows 10					
N/A	2018-12-11	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8641. **CVE ID : CVE-2018-8639**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8639	O-MIC-WIND-201218/38
N/A	2018-12-11	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka "Windows Kernel Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8611	O-MIC-WIND-201218/39

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE ID : CVE-2018-8611**		
Windows 7					
+Info	2018-12-11	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows Server 2012, Windows 7, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8477, CVE-2018-8622. **CVE ID : CVE-2018-8621**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8621	O-MIC-WIND-201218/40
Windows 8.1					
+Info	2018-12-11	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8595	O-MIC-WIND-201218/41

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8596. **CVE ID : CVE-2018-8595**		
Windows Server 2008					
+Info	2018-12-11	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8621, CVE-2018-8622. **CVE ID : CVE-2018-8477**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8477	O-MIC-WIND-201218/42
N/A	2018-12-11	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CV	O-MIC-WIND-201218/43

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8639. **CVE ID : CVE-2018-8641**	E-2018-8641	
+Info	2018-12-11	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8477, CVE-2018-8621. **CVE ID : CVE-2018-8622**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8622	O-MIC-WIND-201218/44
Windows Server 2016					
+Info	2018-12-11	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-201218/45

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8595. **CVE ID : CVE-2018-8596**	guidance/advisory/CVE-2018-8596	
+Info	2018-12-11	2.1	An information disclosure vulnerability exists when Remote Procedure Call runtime improperly initializes objects in memory, aka "Remote Procedure Call runtime Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE ID : CVE-2018-8514**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8514	O-MIC-WIND-201218/46

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.