Vulnerability Type(s)	Publish Date	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
Operating System					
Microsoft					
Windows 10,Windows 7,Windows 8.1,Windows Rt 8.1,Windows Server 2008,Windows Server 2012,Windows Server 2016					
Execute Code	15-08-2018	7.6	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed, aka "LNK Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, 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-2018-8346. **CVE-ID:CVE-2018-8345**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8345	O-Mic-Windo/17-09-18/1
Execute Code	15-08-2018	9.3	A remote code execution vulnerability exists in "Microsoft COM for Windows" when it fails to properly handle serialized objects, aka "Microsoft COM for Windows Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8349	O-Mic-Windo/17-09-18/2
Execute Code	15-08-2018	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka "Microsoft Graphics Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8344	O-Mic-Windo/17-09-18/3

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	Reference/Patch	NCIIPC ID
			Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8344**		
Gain Information	15-08-2018	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 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8394, CVE-2018-8396. **CVE-ID:CVE-2018-8398**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8398	O-Mic-Windo/17-09-18/4
Gain Information	15-08-2018	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 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8396, CVE-2018-8398. **CVE-ID:CVE-2018-8394**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8394	O-Mic-Windo/17-09-18/5
NA	15-08-2018	6.9	An elevation of privilege vulnerability exists in the Network Driver Interface	https://portal.msrc.microsoft.com/en-US/security-	O-Mic-Windo/

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	Reference/Patch	NCIIPC ID
			Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it, aka "Windows NDIS Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8342. **CVE-ID:CVE-2018-8343**	guidance/advisory/CVE-2018-8343	17-09-18/6
NA	15-08-2018	6.9	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior, aka "Windows Installer Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8339**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8339	O-Mic-Windo/17-09-18/7

Windows 10,Windows 7,Windows 8.1,Windows Server 2008,Windows Server 2012,Windows Server 2016

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	Reference/Patch	NCIIPC ID
NA	15-08-2018	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, 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-2018-8399. **CVE-ID:CVE-2018-8404**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8404	O-Mic-Windo/17-09-18/8