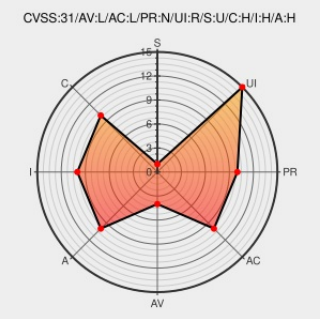
CVE-2018-0598

Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 05/18/2023 04:15:00 PM UTC

CVE-2018-0598

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows from Microsoft contain the following vulnerability:

Untrusted search path vulnerability in Self-extracting archive files created by IExpress bundled with Microsoft Windows allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.

CVE-2018-0598 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Microsoft** - **Self-extracting archive files created by IExpress bundled with Microsoft Windows** version

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
JVN#72748502: Self-Extracting Archive files created by IExpress may insecurely load Dynamic Link Libraries	Third Party Advisory jvn.jp	JVN JVN#72748502

	text/xml	
Triaging a DLL planting vulnerability – Security Research & Defense	Vendor Advisory blogs.technet.microsoft.com text/html	MISC blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-vulnerability/
Triaging a DLL planting vulnerability | MSRC Blog | Microsoft Security Response Center	msrc.microsoft.com text/html	MISC msrc.microsoft.com/blog/2018/04/triaging-a-dll-planting-vulnerability/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→