ALPC Local PrivEsc - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:53:02 UTC

Tool: ALPC Local PrivEsc

Names	ALPC Local PrivEsc
Category	Exploits
Type	0-day
Description	(ESET) On August 27, 2018, a so-called zero-day vulnerability affecting Microsoft Windows was published on GitHub and publicized via a rather acerbic tweet. It seems obvious that this was not part of a coordinated vulnerability disclosure and there was no patch at the time this tweet (since deleted) was published to fix the vulnerability. It affects Microsoft Windows OSes from Windows 7 to Windows 10, and in particular the Advanced Local Procedure Call (ALPC) function, and allows a Local Privilege Escalation (LPE). LPE allows an executable or process to escalate privileges. In that specific case, it allows an executable launched by a restricted user to gain administrative rights.
Information	<https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.alpc_lpe> <https://malpedia.caad.fkie.fraunhofer.de/details/win.powerpool>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool ALPC Local PrivEsc

Changed	Name	Country	Observed
APT groups			

	PowerPool	[Unknown]	2018	

1 group listed (1 APT, 0 other, 0 unknown)
