Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

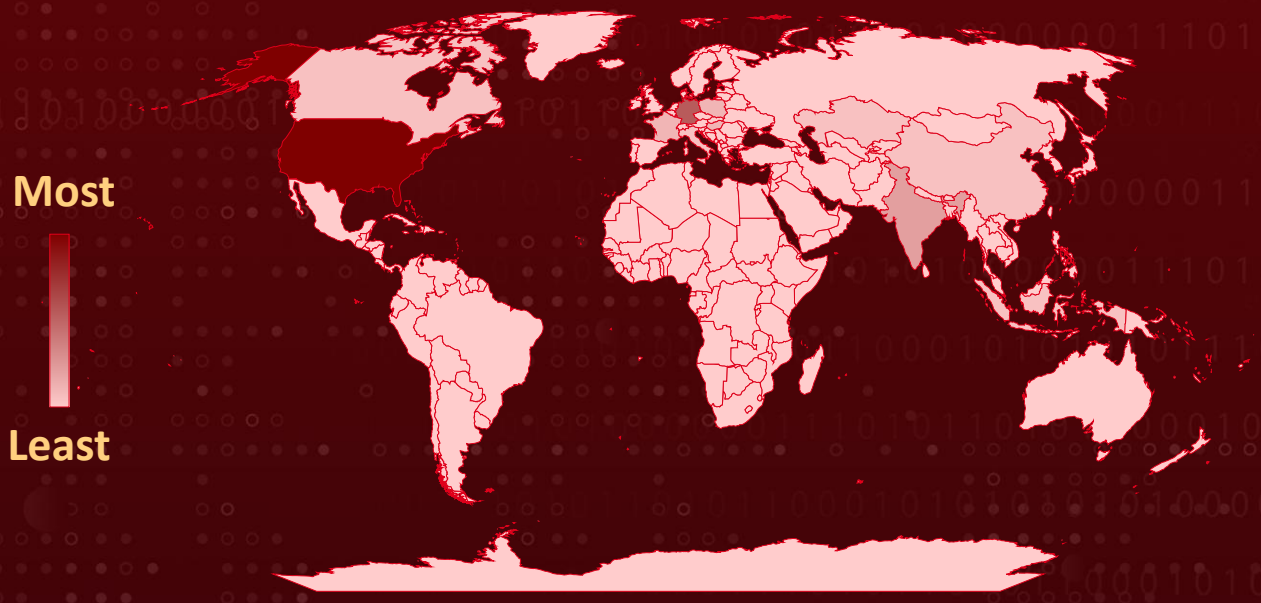
ShadowPad Gatecrashes the Enterprise by Hijacking WSUS Vulnerability

Date of Publication	Admiralty Code	TA Number
November 28, 2025	A1	TA2025363

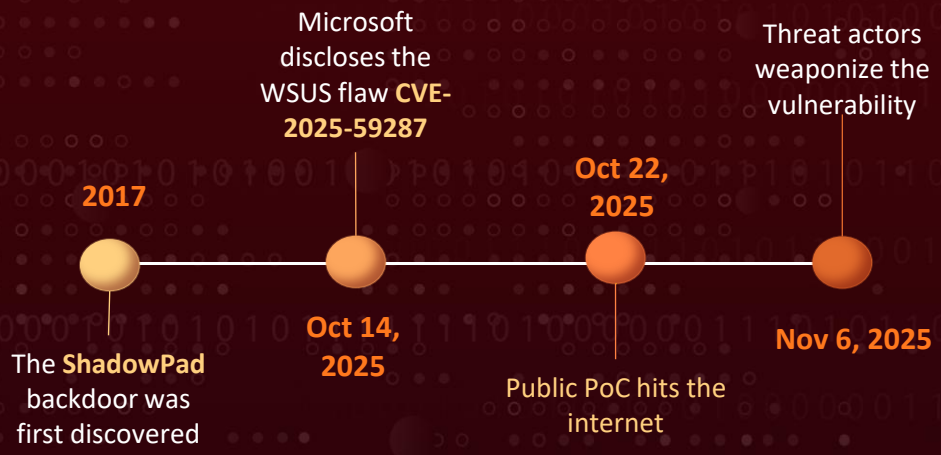
Summary

Attack Commenced: November 6, 2025
Malware: ShadowPad Backdoor
Targeted Region: Worldwide
Affected Platform: Windows
Attack: CVE-2025-59287, a recently patched flaw in Microsoft WSUS, was rapidly weaponized after public exploit code appeared, allowing threat actors to compromise servers and deploy the ShadowPad backdoor used by Chinese state-aligned APT groups. This reflects the high-risk pairing of a critical vulnerability with ShadowPad's persistence and evasion capabilities.

Targeted Regions



Attack Timeline



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-59287	Windows Server Update Service (WSUS) Remote Code Execution Vulnerability	Windows Server Update Service	✗	✓	✓

Attack Details

#1

CVE-2025-59287, a critical vulnerability in Microsoft Windows Server Update Services (WSUS), moved rapidly from disclosure to active exploitation, enabling the delivery of the ShadowPad backdoor. ShadowPad, first identified in 2017, is a modular malware used by multiple Chinese state-backed APT groups. It is privately sold and consistently deployed in long-term espionage operations.

#2

Threat actors began weaponizing CVE-2025-59287 within days of public proof-of-concept code release, focusing on enterprise WSUS environments. Because WSUS servers manage update distribution for large numbers of Windows systems, their compromise provides an ideal foothold for lateral movement and sustained access.

#3

Exploitation follows a structured, multi-stage process. Attackers begin by exploiting the flaw to obtain initial access. After entry, they deploy PowerCat, a PowerShell-based implementation of Netcat. The command observed in the intrusion downloaded PowerCat from GitHub and established a reverse shell to the attacker-controlled infrastructure, granting direct command execution on the compromised server.

#4

The malware deployment phase then uses "living-off-the-land" techniques, relying on built-in Windows tools to retrieve and decode ShadowPad components from a remote host. The overall risk is heightened by the combination of a critical vulnerability, active exploitation by state-sponsored actors, public availability of exploit code, the inherently trusted role of WSUS servers, and the persistence and evasion features embedded in ShadowPad.

Recommendations

Exposure Assessment and Patch Deployment: Identify all Windows Server systems running WSUS and prioritize those reachable from external networks. Apply Microsoft's security update for CVE-2025-59287 immediately.

WSUS Hardening and Access Control: Enforce strict access controls, limiting communication with WSUS servers to Microsoft Update endpoints and authorized internal systems. Block unauthorized inbound traffic on TCP ports 8530 and 8531. Use application whitelisting to prevent execution of unapproved binaries and DLLs on critical systems.

Endpoint and Network Defense Enhancements: Deploy endpoint detection and response tools tuned to identify DLL sideloading and process injection attempts. Monitor for suspicious persistence methods, including services, scheduled tasks, and registry entries referencing "Q-X64" or related identifiers. Inspect network traffic for command-and-control activity disguised with spoofed browser user-agent strings.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**TA0042** Resource Development
T1190 Exploit Public-Facing Application	**T1027** Obfuscated Files or Information	**T1059.001** PowerShell	**T1574.001** DLL
T1574 Hijack Execution Flow	**T1112** Modify Registry	**T1053.005** Scheduled Task	**T1053** Scheduled Task/Job

T1140 Deobfuscate/Decode Files or Information	**T1055** Process Injection	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1218 System Binary Proxy Execution	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1588.006** Vulnerabilities
T1588 Obtain Capabilities	**T1105** Ingress Tool Transfer		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	27e00b5594530e8c5e004098eef2ec50, 564e7d39a9b6da3cf0da3373351ac717, 85b935e80e84dd47e0fa5e1dfb2c16f4, f7d8c52bec79e42795cf15888b85cbad
SHA256	d429934b06de67c156dc559b33c34db5e02bc56ac2c1cd45ee03e6a21cf003af, 3a47e690c47e050125fec16b53ccbbbf722557675f838e5a0fbc1ba1de4ee162
URLs	hxxp[:]//149[.]28[.]78[.]189[:]42306/tmp[.]txt, hxxp[:]//149[.]28[.]78[.]189[:]42306/dll[.]txt, hxxp[:]//149[.]28[.]78[.]189[:]42306/exe[.]txt, hxxp[:]//163[.]61[.]102[.]245[:]443, hxxps[:]//163[.]61[.]102[.]245[:]443
Filename	ETDApix.dll, ETDCtrlHelper.exe, 0C137A80.tmp
File Path	C:\users\%ASD%\tmp.txt, C:\users\%ASD%\dll.txt, C:\users\%ASD%\exe.txt, C:\programdata\0C137A80.tmp
IPv4	154[.]17[.]26[.]41, 149[.]28[.]78[.]189, 163[.]61[.]102[.]245
Mutex	Q-X64

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-59287

References

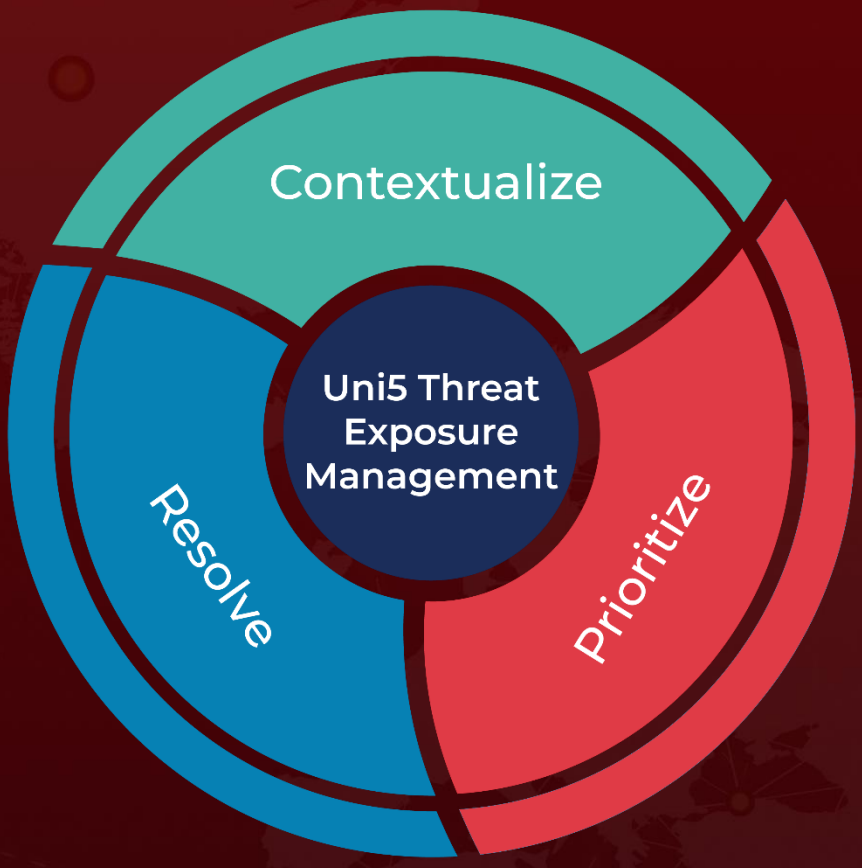
https://asec.ahnlab.com/en/91166/

https://hivepro.com/threat-advisory/microsofts-october-2025-patch-tuesday/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 28, 2025 . 1:00 AM

More at www.hivepro.com