The Tag “Wormable” Should Not Be Totemized — Reflections on the Understanding and Mitigation of RCE Vulnerabilities

This report is a machine-translated version.

1. Introduction

On June 2, 2026, the CleverHans Lab at the University of Toronto, the Vector Institute, and the University of Cambridge (Nicolas Papernot Team) released a preprint titled "AI Agents Enable Adaptive Computer Worms". This paper describes a fully autonomous and adaptive AI worm that does not rely on fixed vulnerability exploits but instead uses real-time inference and customized attack strategies. Its architecture involves running an open-source LLM locally on the compromised machine (without requiring a commercial API) and requesting inference from GPU nodes via weak devices such as IoT devices. In a test environment consisting of 33 hosts (Linux/Windows/IoT), after 7 days and 15 rounds of experiments, it identified 31 valid vulnerabilities/configuration flaws and successfully moved laterally. The study concludes that in AI-enabled scenarios, the marginal cost for attackers is zero, and traditional patch defenses are ineffective; autonomously generated attacks have moved from theory to reality. This research presents a different picture from the previous predictive analysis response of "critical vulnerabilities" to worm propagation.

Starting with the response to the "Code Red II" worm, the Antiy team has been fully involved in the response, analysis, and attribution of dozens of major worms, including "Sasser", "Blaster", "Password Worm", "Mocbot", and "WannaCry". Four months before the

"WannaCry" worm spread using the EternalBlue vulnerability, Antiy also issued a risk warning that ransomware attacks could merge with worms. Antiy CERT , in its recent risk assessment of a series of RCE vulnerabilities, is also reviewing the application of the "wormable" tag for vulnerabilities.

"Wormable" has long been considered a core tag for determining the highest risk level of RCE vulnerabilities in the industry. However, currently, the industry tends to hastily assign this tag based solely on basic attributes in CVSS scoring such as no privilege required (PR:N), no user interaction (UI:N), and network reachability (AV:N). This has led to a "crying wolf" effect, fueled by hype from self-media. Antiy CERT, by comparing two recent Microsoft RCE vulnerabilities, analyzes a reasonable assessment method for "wormable" vulnerabilities and the limitations of the traditional binary perspective.

On April 14, 2026, Microsoft's April Patch Day disclosed the CVE-2026-33827 Windows TCP/IP RCE vulnerability, discovered by the MDASH AI system. This vulnerability, with a CVSS score of 8.1, was flagged as a "wormable" vulnerability by some vendors, including ZDI, due to its unauthenticated remote execution capability. This led to widespread dissemination by domestic security vendors, threat intelligence platforms, and independent media, causing some user panic. However, Microsoft's MSRC gave it a conservative rating of "Exploitation Less Likely", a significant discrepancy from the mainstream tag. A month later, in May 2026, Microsoft's May Patch Day disclosed the CVE-2026-41089 Windows Netlogon RCE vulnerability, with a CVSS score of 9.8. It also features unauthenticated, non-interactive, and network reachable characteristics, relying on the default Netlogon core service enabled

by Windows domain controllers, without additional configuration constraints. Exploitation in the wild has already been detected, making it a typical high-risk "wormable" vulnerability in 2026.

These two high-risk RCE vulnerabilities provide an excellent comparative sample. Based on the analysis of these two vulnerabilities, Antiy CERT traces the definition of the term "wormable", explains the impact of preconditions on vulnerability worm propagation in conjunction with worm propagation conversion rates, analyzes the drawbacks of the traditional binary labeling model, discusses common misconceptions in vulnerability wormable assessment, and proposes a new four-dimensional non-mutually exclusive exploitation model evaluation framework.

2. Tracing the Origins of the "Wormable" Term and the Root Causes of Contemporary Misuse

2.1 Origin of "Wormable"

There is a certain causal dependency between major security vulnerabilities and the emergence of worms. Antiy's overall incident response framework before 2010 was also based on this. Starting in 2004, Antiy CERT, based on the review and summary of multiple rounds of worm incident response, implemented the threat response framework shown in the diagram below. It also listed whether a vulnerability had the potential for autonomous worm propagation as one of the core dimensions of vulnerability risk assessment and issued multiple warnings about the possible emergence of worms, but it did not develop a concise tag like "wormable".

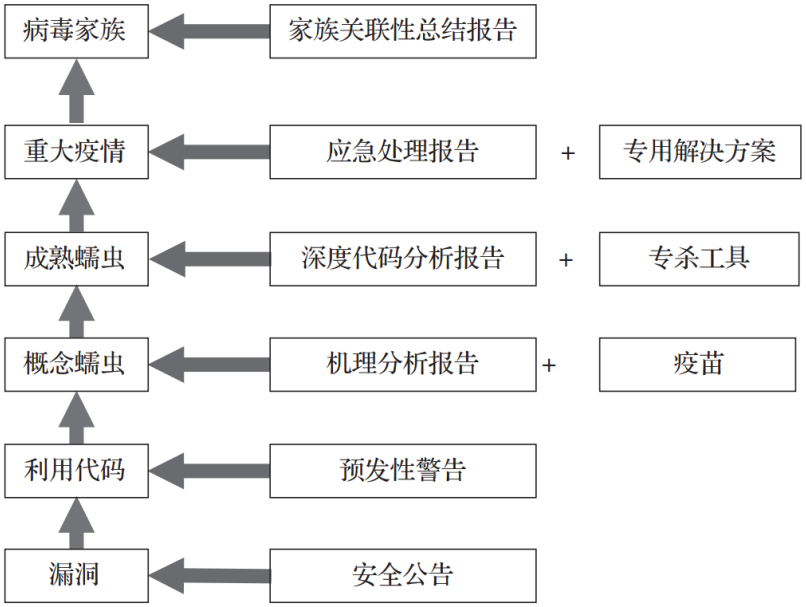

Figure 2-1 Antiy CERT Threat Response Framework (2004)

Microsoft initially used the tag "wormable" in its security advisories, but tracing its etymology, "wormable" is not a rating originally defined by Microsoft. The academic concept was first formally proposed in 2004 by security researchers at UNIRAS and Arbor Networks to **quantify the technical potential of vulnerabilities to be indiscriminately and massively propagated by worms. The core evaluation criteria include three dimensions: propagation stability, target universality, and unrestrained diffusion capability** . In 2019, Microsoft first disclosed "wormable" as an official risk tag in its BlueKeep (CVE-2019-0708) vulnerability announcement. Since then, the term has officially entered the industry's threat assessment discourse from an academic research tag and has gradually become a core tag for the public and security vendors to determine high-risk RCE vulnerability threats.

However, this has led some organizations to directly determine that a vulnerability possesses wormable propagation capabilities based solely on the basic attributes of no

authentication, no interaction, and network reachability in the CVSS dimension, completely ignoring configuration constraints, preconditions for mechanisms, and attack conversion rates in real network environments. We believe that the labeling of CVE-2026-33827 as a "wormable" vulnerability is a manifestation of some organizations' misuse and overgeneralization of the "wormable" concept.

2.2 Prerequisites and Conversion Rate Constraints for Worm Transmission

The effectiveness of worm propagation is not solely determined by "network reachability", but is constrained by the conversion rate. The conversion rate depends on the product of three core variables:

> Conversion Rate Model: Conversion Rate = Addressable Base x Prevalence of Prerequisites x Reachability

All three are indispensable and have a multiplicative relationship—if any variable approaches zero, the overall conversion rate is extremely low, and wormable propagation loses its practical significance. Among them, the target base is determined by the asset penetration rate, reachability is determined by network boundaries and firewall policies, and the degree to which infection conditions are generally met is the most easily overlooked factor in the judgment.

3. Overview of the Two Vulnerabilities and Divergences in Judging the "Wormable" Attribute

3.1 Analysis of the Technical Characteristics of Two High-Risk RCE Vulnerabilities

CVE-2026-33827 and CVE-2026-41089 are both high-risk Remote Code Execution (RCE) vulnerabilities, officially confirmed by Microsoft as critical vulnerabilities. They possess the basic wormable attributes of no authentication, no user interaction, and remote network triggering, but their vulnerability mechanisms, triggering conditions, and application scenarios differ significantly. Specific technical parameters are shown in the table below.

Table 3-1 Comparison of Technical Characteristics of Two High-Risk RCE Vulnerabilities

Parameters	CVE-2026-33827	CVE-2026-41089	Data Source
Vulnerability Name	Windows TCP/IP protocol stack race condition RCE vulnerability	Windows Netlogon protocol stack buffer overflow RCE vulnerability	MSRC, ZDI
CVSS v3.1 Score	8.1 High	9.8 Critical	Tenable, NVD
Core Attributes	AV:N/AC:H/PR:N/UI:N	AV:N/AC:L/PR:N/UI:N	Microsoft official announcement
Difficulty	High (requires competitive conditions to win + environmental configuration)	Low (no special prerequisites)	MSRC, Rapid7
Official Assessment	Less Likely Exploitation	Less Likely Exploitation	Microsoft MSRC
Exploitation in the Wild	No public PoC	Multiple instances of in-the-wild exploitation have been detected.	Brinqa, ZDI
Wormable Tag Determination	Some manufacturers' tags	The industry generally believes it can be "wormable".	Analysis of mainstream security vendors

CVE-2026-33827 is caused by a lack of thread synchronization in the Windows tcpip.sys protocol stack. Attackers need to send concurrent malformed IPv6 fragmented packets to trigger a memory corruption vulnerability. Its core limitations are high attack complexity and dual environmental prerequisites. CVE-2026-41089, on the other hand, is a Netlogon

protocol stack buffer overflow affecting all Windows Server domain controllers. Relying on core services enabled by default, its attack path is simple, highly stable, and requires no configuration, giving it a natural advantage for large-scale propagation.

3.2 Differentiation Analysis of Pre-Constraints for Dual Vulnerability Exploitation

Based on the conversion rate model, the core difference between the two vulnerabilities lies in the number of target systems that can be selected and the degree to which infection conditions are generally met. The stringent preconditions directly determine the hierarchical difference in the worm's propagation ability between the two, forming a clear boundary between true and false worm vulnerabilities.

CVE-2026-33827 Double Strong Constraint Condition:

Effective exploitation of this vulnerability requires simultaneously satisfying two progressive constraints: IPv6 public network reachability and the effective operation of IPsec services. These two conditions have very little overlap in typical public network scenarios. First, regarding IPv6 reachability, while global IPv6 adoption has exceeded 50%, a massive number of terminals are often trapped within NAT systems (including home gateways) and corporate firewalls, lacking public network reachability. Second, regarding IPsec runtime constraints, exploitation requires not only enabling the system's IPsec service but also complex operations such as policy configuration, IKE negotiation, and SA security association establishment. SANS ISC explicitly states that IPsec/IKE services are not enabled by default, and their deployment is not widespread in typical government, enterprise, and

home environments. Furthermore, RCE vulnerabilities typically propagate as worms following a "scan/discover/exploit/deploy" pattern. However, under the IPv6 protocol, the address space expands dramatically. If traditional random scanning strategies are used, most probe requests will target empty addresses (i.e., unallocated or unused address space), leading to a significant decrease in scanning efficiency. Therefore, the fundamentals for scalable propagation of this vulnerability worm are weak.

CVE-2026-41089 Zero-Constraint Exploitation Conditions:

This vulnerability requires no additional environmental or configuration constraints, aligning with the original academic definition of wormable worms. The Netlogon service it relies on is a core foundational service enabled by default on Windows domain controllers. It is enabled by default on all domain servers, widely deployed across the network, requiring no additional configuration from administrators or support for special network protocols. Attackers only need network connectivity to launch indiscriminate remote attacks. The target base is large, the infection conditions are highly satisfied, and the exploitation difficulty is extremely low, fulfilling the core requirements of automated, large-scale, and indiscriminate spread of worms.

3.3 Essential Comparison Between the Two Cases Based on Historical Worm Vulnerabilities

By compiling industry data on wormable vulnerabilities and real-world large-scale propagation events, we can further summarize the characteristics and patterns from

vulnerability discovery to the emergence of large-scale worm events. Some vulnerabilities labeled "wormable" in the past five years (CVE-2019-0708 (BlueKeep), CVE-2020-0796 (SMBGhost), CVE-2022-21907 (HTTP.sys), CVE-2024-38063, CVE-2026-33827) are all in the form of Remote Code Execution (RCE), but none have resulted in a global worm event of the scale of WannaCry. History has repeatedly proven that merely satisfying the "unauthorized remote code execution" condition is far from sufficient to drive automated, self-propelled wormable propagation.

Table 3-2 Comparison of Constraints Between Historical Actual Worm Outbreak Vulnerabilities and "Wormatable" Vulnerabilities

CVE	Name	The Creator of "Wormable"	Has a Large-Scale Worm Outbreak Occurred?	Key limitations
MS03-026	Blaster	/	yes	Port 135/RPC is open by default and requires no authentication.
MS04-011	Sasser	/	yes	LSASS network reachable, no authentication required
MS08-067	Server Service RCE	/	Yes (Conficker, 2008-2009)	Port 445 is open by default, and Server Service is enabled by default.
MS17-010 **CVE-2017-0144**	EternalBlue	NSA / Security Community	Yes—WannaCry began spreading at 7:44 AM UTC on May 12, 2017, and stopped spreading approximately	Port 445 is open by default, SMBv1 is enabled by default, and the Internet is accessible; the NSA's weaponized code leak provides a mature exploit; the ransomware comes with its own propagation module.

			7 hours and 19 minutes after Marcus Hutchins registered the kill-switch domain; ultimately infecting over 300,000 computers (in 150+ countries).	
CVE-2019-0708	BlueKeep RDP RCE	Microsoft (referred to as "wormable" in the announcement) + ZDI	No – Only cryptocurrency mining loads appear (Kevin Beaumont honeypot 2019-11, Kryptos Logic analysis)	RDP (3389) requires administrator activation or exposure; Metasploit module has poor stability; NLA mitigation.
CVE-2020-0796	SMBGhost SMBv3 compression RCE	Security community (the term "wormable" is used for leak notifications)	No – PoC BSOD only, no large-scale worms	SMBv3.1.1 compression was only introduced in Win10 1903/1909, resulting in a narrow version range and low stability.
CVE-2022-21907	HTTP.sys HTTP protocol stack	Microsoft (FAQ acknowledged) + ZDI + SOC Prime	No	HTTP Trailer Support is disabled by default in Server 2019 / Win10 1809; IIS Desktop is not enabled by default; attackers cannot directly obtain kernel read/write primitives.
CVE-2024-38063	IPv6 RCE TCP/IP	ZDI + Security Community	No (no large-scale worm activity was observed)	Integer underflow is mitigated by KASLR/CFG and other methods; reliable RCE is difficult; enterprise export equipment

				filters malicious IPv6 extension headers.
CVE-2026-33827	TCP/IP race condition (IPv6 + IPSec)	ZDI (Vendor Only)	As of May 2026, there has been no field utilization, no publicly available Proof-of-Concept (PoC), and no large-scale worm utilization has been observed.	AC:H race conditions, requires pre-configured environment, IPSec must be enabled and SA established, and the attack source must be within the IPSec domain.
CVE-2026-41089	Netlogon RCE	ZDI	Yes (already being used in the wild).	Netlogon is enabled by default, full coverage of domain controllers, and no prerequisites.

Some security vendors and self-media have compared CVE-2026-33827 to EternalBlue (MS17-010) or earlier vulnerabilities like Blaster and Sasser, which were exploited by large-scale worms in the past. This is an inaccurate analogy.

3.4 Origins and Discrepancies of Vendors' "Wormable" Judgments

There are significant differences in standards among security vendors regarding the assessment of "wormable". Microsoft's MSRC did not use the term "wormable" in its official announcements for either of these vulnerabilities, instead giving it a relatively conservative "Exploitation Less Likely" rating. The "wormable" tag for CVE-2026-33827 originated from a comment by ZDI (Dustin Childs), and other major vendors generally quoted or echoed this assessment in their analyses. However, the "wormable" tag usually attracts media attention and amplification, especially from independent media outlets.

Table 3-3 Vendor-Specific Judgments for CVE-2026-33827 Vulnerability

Vendor/Source	Expression	Basis for Argumentation	Biased Positions
Microsoft MSRC	"wormable" not used; rating: "Exploitation Less Likely"	Strict triggering conditions	Balance
ZDI (Childs)	"That adds up to a wormable bug"	Deducing from attributes	Strong
Tenable	ZDI is described as wormable.	Reprinted from ZDI	Strong
CrowdStrike	Objectively quoting MSRC, without the wormable tag.	Original text transcription	Balance
Cisco Talos	Objectively quoting the explanation of race condition	Original text transcription	Balance
Action1	Listed as Critical, while citing Microsoft less likely	Two positions	Balance
SANS ISC	"never underestimate AI aided attacker"	AI may break through	Cautious

The disagreement surrounding the assessment of the CVE-2026-33827 vulnerability centers on whether "unauthenticated + no user interaction required" is solely a sufficient condition for worm formation. ZDI is keen to label it "wormable", but its reasoning—inferring the likelihood of worm formation from vulnerability attributes (PR:N, UI:N, AV:N)—fails to substantially assess the "target base x prerequisite satisfaction x reachability" required for infection conversion. Microsoft, on the other hand, uses phrases like "Exploitation Less Likely" and "additional preparatory actions" to imply the complexity of race condition exploitation and the difficulty of pre-setting the target environment; the latter is clearly more rigorous.

The mainstream security vendors have different opinions on the CVE-2026-41089 vulnerability, which has stronger wormable characteristics. Some mark it as high-risk, while others mark it as a "wormable" vulnerability. The specific statements from each party are shown in the table below.

Table 3-4 Vendor-Specific Judgments for CVE-2026-41089 Vulnerability

Vendor/Source	Expression	Basis for Argumentation	Biased Positions
Microsoft MSRC	"wormable" not used; rating: "Exploitation Less Likely"	The default enabled Netlogon core service can lead to complete takeover of system privileges.	Balance
ZDI (Childs)	"This vulnerability is wormable"	The default Netlogon service is unauthenticated, has no interaction, is easy to exploit, and has the characteristics of cross-domain lateral propagation.	Strong
CrowdStrike	"Critical Vulnerability in Windows Netlogon "	Confirm its attributes: no authentication, no interaction, and default service enabled.	Strong
Cisco Talos	"critical stack-based buffer overflow in Windows Netlogon"	Original text transcribed from Microsoft	Balance
Action1	" Even though exploitation is assessed as Less Likely, the potential impact is severe "	Confirming its characteristics of no authentication, no interaction, and low barrier to entry.	Balance

The inconsistent and divergent assessments of the two vulnerabilities by vendors ultimately point to the current chaotic state of worm-related vulnerability assessment in the industry: relying solely on basic CVSS attributes as the criterion, ignoring the pre-existing constraints of the real network environment, the exploitation threshold, and the propagation conversion rate, ultimately leading to misclassification and confusion.

4. Deficiencies of the Traditional Wormable Assessment Framework for RCE Vulnerabilities Reflected by the Two Cases

4.1 Historical Causes of Worm Totem Worship

The term "wormable" has been given an almost "totemized" status in the industry's perception—it seems that only when a vulnerability is labeled with this term does it mean that it poses the highest level of threat, but this understanding is not comprehensive.

The Morris-Worm incident of 1988 served as an early warning of threats to the then-nascent internet. It also led to the expectation that major internet threats possess widespread and generalized characteristics. In 2024, Stav Cohe et al., in their CCS2025 paper "Here Comes The AI Worm: Unleashing Zero-click Worms that Target GenAI-Powered Applications", even named their team's concept worm for a self-replicating prompt against a RAG-driven AI email assistant Morris-II. This demonstrates the profound historical impact of the event.

With the accelerated development of the information superhighway by countries around the world in the 1990s, a channel for the global spread of threats was truly provided. Starting with the Happy99 worm on New Year's Day 1999, several waves of worm propagation occurred in the following years. Some email worms relied on manual clicks to run, exhibiting semi-automatic propagation, but more impactful worms such as Code Red, Nimda, SQL Slammer, Blaster, Password Worms, and Sasser achieved autonomous propagation through open ports, service overflow vulnerabilities, weak (empty) password configurations, and zero-click email vulnerabilities. During these large-scale worm

outbreaks, various issues arose, including severe internet congestion, repeated blue screens on some systems (due to different service overflow points in different versions), and the implantation of backdoor programs by some worms. However, from the perspective of most users, the main impact of worms was slow network access, or even complete network unresponsiveness. Because threats are perceptible to the public, they are more likely to attract attention, and the term "worm" is a highly concrete term, making them relatively easy to notice.

Academic research on worms has also served to reinforce labeling to some extent. Because malicious code behaves in a highly complex and varied manner on the system side, and worm propagation behavior can be easily collected and extracted from observational data such as network traffic and system logs, it can also be mathematically modeled based on topology, stochastic processes, and even incorporating biological viral propagation principles. Therefore, worms have been a relatively productive area for papers related to cybersecurity threats for a considerable period.

4.2 Causes and Threat Trends of the "Worm" Surge at the Beginning of This Century

The large-scale spread of worms between 1999 and 2025 was characterized by its specific phases, a unique product of multiple historical factors. These included the rapid construction of the global information superhighway, the relatively weak security of mainstream operating systems (Windows) and the imperfect vulnerability response and repair mechanisms, and attackers' pursuit of psychological satisfaction. In terms of both context and motivation, it was a replay and amplification of the rise of infectious viruses in

the disk era. However, as the internet carries more information value and applications, the driving force of psychological satisfaction in cyberattacks was quickly replaced by profit-driven motives.

Wormable propagation, due to its ease of rapid detection, coordinated triggering, and large-scale handling, is often not considered a preferred method by attackers from a "profit" perspective. RCE vulnerabilities are increasingly being used by attackers for controlled botnet proliferation, particularly in scenarios with higher deterministic returns, including targeted attacks (such as APT attacks) and targeted ransomware (Big Game Hunting). Attackers can achieve penetration, persistence, and data theft before the vulnerability patching window by precisely selecting high-value targets, yielding returns far exceeding the "lottery-like" rewards of indiscriminate worm scanning. Even in the later stages, after vulnerabilities have been publicly disclosed and many users have patched them, gray and black market actors prefer to use them for botnet node expansion rather than open worm exploitation.

From a security perspective, major operating system vendors subsequently improved their buffer overflow protection capabilities through DEP and ASLR, provided more protection for critical applications such as email clients and browsers, and offered compilers more robust memory safety options. Host system security products also evolved from traditional file detection and antivirus to full-featured proactive protection EPP and EDR software, all of which effectively curbed worm propagation. This also made RCE vulnerabilities from mainstream vendors a scarce resource for a considerable period.

The 2017 WannaCry worm incident, driven by the economic model of this new threat—ransomware attacks—resulted from a shadow broker leaking NSA zero-day exploit tools, leading to the short-term exposure of RCE resources. The attacking group attempted to maximize its "residual value" harvest in a short period. Currently, worm threats are back on the priority list, primarily due to AI-powered vulnerability discovery, allowing attackers to continuously add high-risk RCE vulnerabilities to their arsenals. Simultaneously, AI-assisted decision-making is reshaping worm attack patterns. Worms have shifted from rapidly spreading based on the exposure of a single major vulnerability to a more intelligent model involving vulnerability selection, combination of vulnerabilities, and propagation orchestration. This is a potential risk that requires vigilance.

4.3 Inherent Defects and Causes of Misjudgment in Traditional Binary Classification

However, we must point out that viewing "worm" propagation as the primary perspective reflects a security view specific to the communications era, not the era of complex systems. It inherently carries the misconception that the dominant factor in a threat is simply a topology-based diffusion process, rather than the acquisition and impact on secrets, data, business operations, and assets. Its focus is entirely on the propagation behavior, neglecting the essential nature of "worms" as a type of malicious code.

The binary tag of "wormable" and "non-wormable" has become increasingly one-sided and limited in complex attack and defense environments. First, it focuses solely on the vulnerability's ability to spread over public networks, ignoring its actual exploit value in private networks, intranets, and VPN-isolated environments. Second, it hastily classifies

vulnerabilities based solely on CVSS attributes (no authentication, no interaction, network reachability) without considering pre-existing constraints, configuration thresholds, and conversion rates in real-world environments. Third, it easily triggers labeling panic, leading to a misallocation of protection resources: overemphasizing the risk of public network worms while underestimating the real threats of targeted penetration and lateral movement within intranets. Fourth, it fails to adapt to the complexity of actors/attack activities/attack payloads/attack entry points—attackers combine multiple vulnerabilities, and the same vulnerability can be reused by multiple types of attackers; the binary tag cannot cover diverse application scenarios.

For critical information systems, the more lethal threat has always been covert, targeted attacks, rather than widespread worm propagation. The hype surrounding "wormable" is more likely to create a paralyzing effect through repeated crying of the wolf.

4.4 Objective Potential of Worm Vulnerabilities and Uncertainties in Subjective Exploitation

The core variable in vulnerability exploitation is the subjective decision-making of the threat actor. Whether a vulnerability has the potential for wormable technology and whether it will actually spread in a wormable manner are two highly related but independent judgment dimensions: the former is an objective technical judgment based on vulnerability mechanism and environmental constraints, while the latter is a subjective behavioral prediction that combines attacker motivation, cost-benefit analysis, and attack strategy. The

uncertainty of behavioral prediction is far higher than that of vulnerability technical attribute judgment.

The cyber threat ecosystem comprises numerous threat actors with entirely different objectives, capabilities, and operational mechanisms. These include geopolitical threat actors with national/regional backgrounds, cybercrime organizations, and individual attackers. Different actors have vastly different operational motivations and target selection tendencies, basing their choices on cost-effectiveness. This subjectivity means that the potential for vulnerabilities to be wormed does not necessarily imply a causal relationship between their potential and the inevitable development of worms.

4.5 Prediction of Four Exploitation Modes of RCE Vulnerabilities

Antiy recommends updating the traditional "wormable" binary tag to evaluate the following four non-exclusive exploitation methods:

Mode 1: Wormable Exploitation. This refers to vulnerabilities that can be used to build malicious code that spreads autonomously without human intervention, enabling exponential proliferation in open networks. Its core characteristics are low barrier to entry, high conversion rate, and indiscriminate target selection.

Mode 2: Botnet Augmentation. This refers to the use of vulnerabilities to expand the number of controllable nodes based on an already controlled infection chain, including lateral movement within specific network boundaries (such as an already compromised VPN or internal network segment). This mode does not require propagation over the open

internet, but it requires the vulnerability to be able to be embedded as an automated payload into an existing botnet infrastructure.

Mode 3: Targeted Network Attack. This refers to vulnerabilities being used by APT groups or highly skilled attackers for precise penetration of specific high-value targets, often in combination with prior reconnaissance, social engineering, or other vulnerabilities.

Mode 4: Internal Exploitation. Vulnerabilities can only be triggered within a specific network boundary (such as lateral movement within an intranet after initial access has been gained), or require specific internal knowledge (such as VPN topology, certificate configuration) to be exploited.

Table 4-1 Vulnerability Adaptation Table for Four Non-Mutual Exclusive Exploitation Modes

Model	Spread Range	Target Selection	Prerequisites	CVE-2026-33827 Compatibility	CVE-2026-41089 Compatibility
Wormable Exploitation	Open Internet	Indifference	Low barrier to entry, high conversion rate	Not satisfied	Potential adaptation
Botnet Augmentation	Within the controlled boundary	Semi-directional	A foothold must already be established.	Potential adaptation	Highly adaptable
Targeted Network Attack	Specific high-value targets	Precision	Preliminary reconnaissance is required.	Highly adaptable	Highly adaptable
Internal	Internal	Restricted	Internal	Adaptation	Highly

Exploitation	network/virtual network		access required		adaptable

It should be emphasized that the above four modes are not mutually exclusive, and the same vulnerability may apply to multiple modes at the same time.

4.6 The Scenario Value and Governance Implications of Multi-Modal Analysis

The proposed method for assessing and predicting four exploitation methods for RCE vulnerabilities is an extension of the "wormable" judgment, incorporating motivation and scenarios. It adapts to the dual needs of modern attack and defense scenarios and network governance systems, enabling refined and layered assessment of vulnerability risks. From the core logic of the assessment, the implementation of vulnerability threats always involves both objective technical conditions and subjective attack behavior uncertainties. The inherent mechanism, environmental constraints, and open conditions of the vulnerability itself are fixed and measurable objective facts that determine the upper limit of the vulnerability's potential; while the attack motivations, cost-benefit considerations, and irrational attack behaviors of different types of threat actors directly determine the actual transformation form of the vulnerability. Diverse attacker groups do not have a unified, fully predictable exploitation logic. Even if a vulnerability does not possess complete wormable technical conditions, it may still be exploited on a large scale in specific scenarios; conversely, high-risk vulnerabilities with the ability to spread like worms across the entire network may abandon indiscriminate dissemination and turn to high-value, precise attacks due to attackers' targeted profit demands. This complexity of the misalignment between subjective

and objective factors thoroughly confirms the core pain point that traditional binary tags cannot adapt to modern vulnerability risk assessment, and also highlights the necessity of multi-mode assessment and judgment.

From a real-world scenario perspective, vulnerability assessment and security governance naturally differ in their perspectives: public regulatory scenarios and enterprise defense scenarios. The protection objectives, risk thresholds, and handling priorities of these two scenarios are quite different, and precise adaptation can be achieved by relying on four exploitation modes.

For public network regulators, the long-term focus on the large-scale network-wide consequences of wormable exploitation is due to the fact that this model is characterized by open internet spread, indiscriminate attacks, and exponential proliferation, which easily puts pressure on public networks and is a key area for public security prevention and control. However, the cost and difficulty of detecting it from the regulatory side are relatively low. On the other hand, targeted network attacks and internal exploitation have low public network awareness and weak risk of network-wide spread, making them extremely difficult to detect from the regulatory side and requiring greater collaboration between government agencies, enterprises, and security companies.

For enterprise-level defense, the perspective is completely reversed. Regardless of whether a vulnerability has the capability for public network worm propagation, as long as it can achieve targeted penetration, lateral movement within the internal network, node privilege expansion, and asset control, it will cause substantial harm to the enterprise's core business,

data assets, and network boundaries. The final asset losses and business disruptions caused by attackers using different methods are essentially the same. Therefore, enterprise defense does not need to overly focus on the "wormable" tag. For each major vulnerability, the focus should be on whether it exists internally, whether it is usable by attackers, and how to prevent attackers from using it. This involves combining host antivirus protection, hot patch emergency protection, network domain isolation, access control, and traffic auditing capabilities to achieve scenario-based governance.

5. Conclusion: Avoid Vulnerability Panic and Use Defense-in-Depth to Block Vulnerability Exploitation

Through a comparative analysis of two high-risk RCE vulnerabilities, CVE-2026-33827 and CVE-2026-41089, we have outlined the historical significance of the "wormable" tag and the cognitive interference it currently causes. This tag was once second only to zero-day (undisclosed) vulnerabilities in terms of its "totemized" significance. It is noteworthy that both high-risk vulnerabilities used in this comparison are typical "delayed exposure vulnerabilities", with official patches released more than a month before their disclosure. Users who patched them promptly were unaffected, while the risk lay with users and enterprises who delayed or refused patch updates. The industry focuses on discovering "undisclosed vulnerabilities" while neglecting to patch or address a large number of zero-day vulnerabilities—a widespread reality. As a team that experienced real-world threat responses in the early 21st century, we deeply understand that security evolution relies on solid, rigorous, and systematic work, not on the "totemized" treatment of threats and risks.

Only by abandoning the worship of "wormable" and zero-day vulnerabilities can we better carry out our work.

The effectiveness of vulnerability exploitation depends heavily on the fulfillment of a series of preconditions. Therefore, vulnerability response strategies are based on a hierarchical system that includes: increasing the difficulty of detection (security gateways, exposure surface management, fingerprint obfuscation, etc.), increasing the difficulty of exploitation (domain control, expanding the scope of DEP and ASLR protection, etc.), eliminating the root cause (timely patch updates and hot patching, etc.), and mitigating the consequences (intercepting exploit payload distribution, intercepting attack execution, controlling the behavior of the execution, controlling lateral movement, etc.).

For example, regarding the protection against the CVE-2026-33827 worm risk: the core approach is to block dual preconditions. At the network layer, filter IPv6 fragmentation header traffic and disable unnecessary IPv6 fragmentation reassembly. At the service layer, restrict IPsec service permissions, limit UDP port 500/4500 access, and only allow trusted network segments to negotiate SA security associations. At the business layer, directly disable IPsec services for terminals and servers without IPsec services, completely eliminating attack triggering conditions. Regarding the protection against the CVE-2026-41089 worm risk: the core approach is to strengthen overall protection and focus on hardening domain controllers. The perimeter firewall restricts access permissions for unknown IPs to domain controller servers; all domain controller nodes are hardened promptly, and abnormal Netlogon service traffic is monitored; a dedicated domain

environment inspection mechanism is established to prevent automated worm scanning and mass intrusion.

The key reason we've restarted this discussion is that with AI's large-scale empowerment of vulnerability discovery, the continuous and even mass exposure of major vulnerabilities will become the norm, making it unrealistic to continue with an incident-driven response approach. AI-enabled cyberattacks will significantly alter the logic of vulnerability exploitation. Attackers will more frequently use AI-orchestrated combinations of multiple vulnerabilities and differentiated exploitation against different targets. More attack payloads will possess agent-like attributes, evolving and growing on their own after deployment. This is unprecedented. This necessitates stronger defenses against attack payloads. Antiy CERT reiterates that attempting to eliminate threats by "exhaustively discovering vulnerabilities" or designing systems without vulnerabilities is unrealistic . Attacker exploitation is a chain of actions with a series of prerequisites, and every chain has both its strengths and weaknesses. Defenders must disrupt this chain, focusing on the executor as the key defense target.

In the new normal of the rapid popularization of AI vulnerability discovery technology and the mass outbreak of high-risk RCE vulnerabilities, security companies need to avoid becoming "unprofessional" self-media outlets and reduce the habitual behavior of labeling and selling panic. The defense side needs to move beyond the old model of reactive, vulnerability-information-driven responses. This paper proposes a four-dimensional non-mutually exclusive exploitation model assessment perspective to accurately analyze the

differentiated threats such as public network spread, internal network penetration, targeted attacks, and botnet expansion, improving the vulnerability assessment mechanism from the perspectives of motivation and scenario matching. We will further refine the methodology.

Reducing the inherent vulnerability of a scenario and mitigating external threats are two related but independent tasks. For over 20 years, Antiy's core work has focused on providing common threat detection capabilities. In the era of AI+, we continue to empower ecosystem partners and users to combat both new and existing threats in new scenarios.

Reference Link

[1]CleverHans Lab. AI Agents Enable Adaptive Computer Worms[EB/OL]. (2026-06-2)

https://cleverhans.io/worm

[2] Antiy. "IIS Worm: Code Red"

(Published in Antiy Technical Articles Compilation (Part 3))

[3] Antiy. "Emergency Worm.Dvldr Situation Analysis Report" and "Worm Family Association Analysis Report Based on Password Cracking Mechanism"

(Published in Antiy Technical Articles Compilation (Part 3))

[4] Antiy. "Virus Homology Analysis Based on Typical Development Methods and Coding Psychology"

(Published in Antiy Technical Documentation Compilation (Part 1))

[5] Antiy. "Antiy In-Depth Analysis Report on WannaCry Ransom Worm"

https://www.antiy.com/response/wannacry.html

[6] TechJack Solutions. Microsoft MDASH AI Discovers Two Critical RCE Flaws in Windows IKEv2 and TCP/IP Stacks (CVE-2026-33824, CVE-2026-33827)[EB/OL]. (2026-05-13).

https://techjacksolutions.com/scc-intel/microsoft-mdash-ai-discovers-two-critical-rce-flaws-in-windows-ikev2-and-tcp-ip-stacks-cve-2026-33824-cve-2026-33827/

[7]IntegSec. CVE-2026-33827: Windows TCP/IP Race Condition - What It Means for Your Business and How to Respond[EB/OL]. (2026-04-19).

https://integsec.com/blog/cve-2026-33827-windows-tcp-ip-race-condition-what-it-means-for-your-business-and-how-to-respond

[8]Action1. CVE-2026-33827 – Windows TCP/IP Remote Code Execution Vulnerability[EB/OL]. (2026-04-14).

https://www.action1.com/vulnerabilities/cve-2026-33827/

[9]Computerworld. Microsoft's Patch Tuesday release for April is a whopper[EB/OL]. (2026-04-17).

https://www.computerworld.com/article/4160481/microsofts-patch-tuesday-release-for-april-is-a-whopper.html

[10]CrowdStrike. April 2026 Patch Tuesday: Updates and Analysis[EB/OL]. (2026-04-14).

https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-april-2026/

[11]SANS ISC. Microsoft Patch Tuesday April 2026[EB/OL]. (2026-04-14).

https://isc.sans.edu/diary/32898

[12]Brinqa. The New Normal: Volume Is Elevated, AI Is In the Stack[EB/OL]. (2026-05-19).

https://www.brinqa.com/blog/may-2026-vulnerability-analysis-patch-tuesday-ai-security

[13]CVEfeed.io. CVE-2026-33827 Detail[EB/OL]. (2026-04-17).

https://cvefeed.io/vuln/detail/CVE-2026-33827

[14]SentinelOne. CVE-2026-33827: Windows TCP/IP Race Condition Vulnerability[EB/OL]. (2026-04-17).

https://www.sentinelone.com/vulnerability-database/cve-2026-33827/

[15]Tenable. CVE-2026-33827[EB/OL]. (2026-04-14).

https://www.tenable.com/cve/CVE-2026-33827

[16]Zero Day Initiative. The April 2026 Security Update Review[EB/OL]. (2026-04-14).

https://www.thezdi.com/blog/2026/4/14/the-april-2026-security-update-review

[17]APNIC Blog. Google hits 50% IPv6[EB/OL]. (2026-04-28).

https://blog.apnic.net/2026/04/28/google-hits-50-ipv6/

[18]Internet Society Pulse. 18 Years Later, IPv6 Reaches Majority[EB/OL]. (2026-04-21).

https://pulse.internetsociety.org/en/blog/2026/04/18-years-later-ipv6-reaches-majority/

[19]Cisco Blogs. IPv6 in 2025 – Where Are We?[EB/OL]. (2025-05-07).

https://blogs.cisco.com/industries/ipv6-in-2025-where-are-we

[20]Penta. Revisiting the WannaCry Ransomware Attack[EB/OL]. (2025-04-03).

https://penta.ch/insights/revisiting-the-wannacry-ransomware-attack-how-to-stay-protected

[21]Cloudflare. What was the WannaCry ransomware attack?[EB/OL].

https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

[22]Windows Forum. KB5091157 April 2026 Out-of-Band Fix for Windows Server 2025 Reboot Loops[EB/OL]. (2026-04-20).

https://windowsforum.com/threads/kb5091157-april-2026-out-of-band-fix-for-windows-server-2025-reboot-loops.414371/

[23]Action1. CVE-2026-33824 – Windows IKE Service Extensions RCE[EB/OL]. (2026-04-14).

https://www.action1.com/vulnerabilities/cve-2026-33824/

[24]Windows Forum. WinRE Startup Fix: March 2026 KB5075039[EB/OL]. (2026-03-06).

https://windowsforum.com/threads/winre-startup-fix-march-2026-kb5075039-resolves-october-2025-regression.404183/

[25]Hackread. Pwn2Own Berlin 2026 Hits Capacity as Rejected Hackers Release 0-Days[EB/OL]. (2026-05-12).

https://hackread.com/pwn2own-berlin-2026-hits-capacity-hackers-0-days/

[26]HelpNetSecurity. AI shrinks vulnerability exploitation window to hours[EB/OL]. (2026-05-18).

https://www.helpnetsecurity.com/2026/05/18/synack-2025-ai-driven-vulnerability-trends-report/

[27]Trend Micro. Fault Lines in the AI Ecosystem: TrendAI State of AI Security Report[EB/OL]. (2026-03-03).

https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/fault-lines-in-the-ai-ecosystem-trendai-state-of-ai-security-report

[28]HAL. Cyber Weather Forecasting: Forecasting Unknown Internet Worms Using Randomness Analysis[EB/OL]. (2017.5.4).

https://inria.hal.science/hal-01518242v1/document

[29]semantic scholar. Wormability: A Description for Vulnerabilities[EB/OL]. (2024).

https://www.semanticscholar.org/paper/Wormability%3A-A-Description-for-Vulnerabilities-Nazario-Ptacek/48819461fefae32c189e15ae035dbfd0428c2bb8 #paper -topics

[30]Microsoft. Windows Netlogon Remote Code Execution Vulnerability[EB/OL]. (2026.5.12).

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089

[31]ZDI. The May 2026 Security Update Review. [EB/OL]. (2026.5.12).

https://www.zerodayinitiative.com/blog/2026/5/12/the-may-2026-security-update-review

[32]action1. CVE-2026-41089 – Windows Netlogon Remote Code Execution Vulnerability[EB/OL]. (2026.5)

https://www.action1.com/vulnerabilities/cve-2026-41089/

[33]Stav Cohen, Ron Bitton, Ben Nassi. Here Comes The AI Worm: Unleashing Zero-click Worms that Target GenAI-Powered Applications(2025.1.30).

https://arxiv.org/abs/2403.02817