Number 114 | May 2026

NTT DATA

Radar

The Cybersecurity Magazine

Beyond the Algorithm: Reinventing CTI in an Era of Democratized Attacks

By Alexis Martín García

As intelligence professionals, we often say that our job is fundamentally about reducing uncertainty to support decision making. However, in the most recent cycle, that uncertainty has not only evolved, it has also reached a velocity that challenges our traditional defense models. We are no longer facing only state sponsored groups with virtually unlimited resources or the opportunism of conventional cybercrime; we are witnessing a democratization of offensive capabilities that has upended the rules of engagement as we knew them just a few months ago.

The reality on the operational front lines is that the barrier to entry for the adversary has collapsed. The rise of offensive automation and the use of language models applied to malware development have transformed the economics of attack: today, the cost of execution for the attacker is approaching zero, while the cost of defense for organizations remains linear and continues to grow. Any actor with clear intent can now generate polymorphic payloads capable of evading signature based endpoint solutions, or design social engineering campaigns so precise that the human factor is left completely exposed. We have moved from detecting textbook attacks to managing a symphony of automated noise that, with algorithmic persistence, searches for that single forgotten asset within our exposure surface or that newly disclosed zero day vulnerability.

In this saturated environment, traditional indicators of compromise, those IPs, domains, and hashes that used to form the backbone of our operations, have become ephemeral assets. Their lifespan in today's ecosystem is so short that by the time they reach our blocklists, the adversary has already rotated its command and control infrastructure. For this reason, the focus of modern intelligence must inevitably shift toward the analysis **of TTPs, tactics, techniques, and procedures.** Understanding modus operandi and behavioral patterns is no longer an academic exercise, but the only realistic way to anticipate an access vector before it becomes an incident with systemic impact.

But this technological arms race is not one sided. We, as defenders, have also enhanced our response capabilities through the same technology that challenges us. The integration of artificial intelligence and machine learning into the CTI workflow is allowing us, for the first time, to process telemetry and open source intelligence at a scale that until recently was purely theoretical. We are now able to connect seemingly isolated data points between a trivial network event and a targeted campaign that is still in its reconnaissance phase. The ability to filter noise and prioritize threats based on actual risk is what enables our response teams to avoid succumbing to alert fatigue.

It is there, in the detection of invisible patterns and in the orchestration of intelligence, where our discipline becomes the most critical strategic asset. What you will find in the pages of this edition is a journey through the multidimensional nature that defines modern CTI, from the weight of global realities and the tensions that shape strategic objectives, to the technical sophistication that enables initial compromise, concluding with the trends that are redefining our operational roadmap. It is not just about accumulating data, but about transforming it into actionable knowledge that allows the organization to stay one step ahead on the board.

In the end, although technology provides the speed and raw processing power needed to navigate this new environment, **the analyst's judgment**, that unique ability to interpret intent, geopolitical context, and the psychology behind the data, remains our final and most resilient stronghold. AI can automate discovery, but only the human analyst can give it meaning. Welcome to an in depth analysis of our most pressing present, where intelligence is, more than ever, the difference between resilience and compromise.

Alexis Martín García
Project Manager of Cyber Threat Intelligence & Hacking Center

When Trust Becomes the Perimeter: Anatomy of a Month of Attacks

Cyber Chronicle by Eduardo Gil Ciruelos

The period from mid March to mid April 2026 did not produce a single historic attack, but something more unsettling: a sequence of incidents that, when read together, precisely illustrate the scenario anticipated in the previous article. The barrier to entry for the adversary has collapsed, automation has accelerated operational cycles, and in parallel, organizations have discovered that their perimeters are no longer where they believed them to be. This is the chronicle of those weeks.

It all began, or at least became visible, on **March 11**. At five in the morning UTC, **Stryker** employees across seventy-nine countries watched their devices shut down simultaneously**. A group linked to Iran** had compromised a single **Microsoft Intune** administrative account, created a new global administrator, and used the legitimate tool to wipe two hundred thousand devices. There was no malware, no ransomware, no binary to analyze. The system did not detect an attack because, technically, it was not seeing one, it was seeing an administrator doing their job

A few days later, the focus shifted to **Crunchyroll**, although the origin of the incident lay much farther away. A support agent at **Telus International,** working from a laptop in India, fell for a phishing email. The captured credentials opened access, via Okta single sign on, to Zendesk, Slack, Workspace, and Jira. In less than twenty-four hours, **one hundred gigabytes of data and nearly seven million email addresses were exfiltrated**. By the time the security team managed to revoke access, the operation was already complete. The perimeter that was breached was not in Tokyo or California, but in an outsourcing contract

While those cases were making headlines, another surfaced with delay. **Marquis Software Solutions**, a service provider for hundreds of financial institutions in the United States, disclosed in March an incident that had occurred seven months earlier. A compromised **SonicWall** firewall had enabled the deployment of ransomware that ultimately affected seven hundred thousand individuals and seventy-four banks. For more than half a year, the victims did not know they needed to protect themselves.

Almost in parallel**, Sapienza University of Rome,** with its one hundred and twenty thousand students, woke up without digital services. Exams, email, administrative processes. Everything halted for several days. There was no immediate claim of responsibility and no major public demands, only the realization that a single compromised entry point was enough to bring an entire institution to a standstill.

The first week of April brought a different kind of shift. On April 7, the **Smart Slider 3 Pro** plugin, present in more than eight hundred thousand **WordPress** installations, released a new version through its official channel. For six hours, that version was in fact a full backdoor written by an attacker who had taken control of the update infrastructure. Every site that updated within that window automatically became a remote access point.

Two days later, the pattern repeated under a different name. **On April 9,** the official download links for **CPU Z and HWMonitor** on the CPUID website began redirecting to malicious domains. The tampering lasted around nineteen hours. The signed binaries themselves remained legitimate, but the website distributing them no longer was. Users who were doing exactly the right thing, downloading from the official source, ended up compromised anyway.

During those same days, the focus shifted to the Latin American public sector. **In Mexico**, a breach in the **Safe Smart Port** system of the Secretariat of the Navy exposed nearly forty gigabytes of information on six hundred and forty thousand port workers, including biometric traits, blood type, and workplace location. The breach did not only compromise personal data, but also the operational traceability of critical logistics infrastructure.

In Argentina, the group Chronus Team had announced days earlier on social media that it would carry out an attack. And it did. Twenty eight simultaneous leaks targeting national and provincial government agencies, as well as health, finance, and security institutions. The prior warning did not trigger any visible coordinated response.

The end of the month was marked by incidents in the private sector. **Adobe** confirmed the exposure of thirteen million support tickets, fifteen thousand employee records, internal documents, and full submissions from its bug bounty program. The sensitivity of the dataset was not in each individual element, but in what could be reconstructed by correlating them.

And on April 11, the group ShinyHunters claimed responsibility for two nearly consecutive operations: at Rockstar Games, the compromise of Snowflake instance metrics through integration with Anodot; at Abrigo, the exfiltration of more than 1.7 million Salesforce records. In neither case did access originate from the final target, but rather from a connected service.

Looking at the month as a whole, the thread that ties all these incidents together is not technical. None required extraordinary capabilities. What connects them is the way each attacker found a trust relationship, a credential, a provider, a signed update, a SaaS integration that the organization had long stopped questioning. None broke down a door. They all had a key.

Eduardo Gil Ciruelos
Junior Cyber Threat Intelligence Analyst

When conflict is not declared: cyberspace as a tool of geopolitical power

Article by Sandra Somastre

Cyberspace has become a domain of geopolitical competition where states project power without the need for direct confrontation. In this environment, cyber operations are not isolated events, but part of broader strategies aimed at persistence, influence, and gaining advantage.

Understanding current threats requires going beyond technical data and analyzing the strategic context in which they develop.

The current geopolitical context is characterized by constant competition among states with increasingly well defined strategic interests.

Far from traditional models of confrontation, conflicts no longer unfold only in the physical domain, but extend into other areas where pressure can be applied in a sustained way and with a lower risk of escalation.

In this context, cyberspace has established itself as an essential vector for projecting power. It is not an autonomous environment, but rather a space where many of today's geopolitical dynamics are shaped: economic pressure, technological rivalry, influence operations, and intelligence gathering.

Cyberspace no longer accompanies conflict: it is part of it by design.

An environment of persistent competition

The international balance has evolved into a more fragmented model, where multiple state actors compete without a clear separation between periods of peace and conflict.

This situation encourages continuous activity in which operations do not necessarily seek immediate impact, but rather aim to position themselves strategically. This logic is ideally suited to activity in cyberspace, enabling sustained action without resorting to traditional methods of confrontation.

Conflicts such as the war between Russia and Ukraine, tensions in the Middle East, and technological competition between China and the West reflect this evolution. In all of them, the cyber component forms a structural part of the conflict, complementing other forms of pressure.

In addition, this model introduces a key feature: **asynchrony.** While traditional conflicts have identifiable phases, activity in cyberspace does not stop. Even in moments of apparent stability, operations continue, accumulating access, information, and capacity for influence.

Cyberspace as a tool of strategic pressure

The value of cyberspace in the current context lies in its ability to operate in what are known as **gray zones of conflict.** In other words, it enables actions that create impact without crossing thresholds that would trigger a direct response, which makes it particularly effective in a geopolitical environment where open escalation carries a high cost.

This logic is not merely theoretical, but is directly reflected in major international scenarios, where this activity accompanies, amplifies, and even prevents conflicts.

In this sense, it is possible to identify different patterns in the use of cyberspace depending on the geopolitical context:

- **Russia and Ukraine:** Cyber activity has been structurally integrated into the conflict, combining influence operations, campaigns targeting third countries, and the disruption of services. Cyberspace makes it possible to extend the reach of the conflict without the need for traditional escalation, generating impact on allies, supply chains, and public opinion.
- **Middle East, including Israel and regional actors:** In this scenario, cyberspace acts as a means of indirect confrontation. Disinformation campaigns, leaks, and coordinated attacks are combined with ideologically aligned hacktivist operations. The objective is not only technical, but also to shape public perception and increase pressure during periods of tension.

- **China and the West:** Activity focuses on cyber espionage campaigns targeting critical sectors such as technology, energy, and advanced manufacturing. This approach reflects a long-term strategy in which information gathering and technological positioning take priority over immediate disruption.
- **United States:** Its role in the digital economy and its geopolitical weight are evident in how cyberspace is used to influence areas where global advantage is determined, from economic stability to innovation, as shown by the concentration of activity in strategic sectors.
- **Iran and North Korea:** These actors combine influence operations, espionage, and activities aimed at resource acquisition. Cyberspace becomes a tool to overcome structural constraints, especially in the economic domain, and to extend their capabilities beyond national borders.

In summary, these scenarios reveal a clear trend: cyber operations are not isolated incidents, but part of ongoing strategies **aimed at exerting influence, wearing down adversaries, and positioning actors within a context of constant competition.** Their impact is not measured only in technical terms, but also by their ability to integrate into broader processes and generate cumulative effects over time.

Technical evolution as a reflection of context

The rise of techniques based on identity exploitation, the use of legitimate tools, and the decline of conventional malware reflect not only operational evolution, but also adaptation to the geopolitical environment. In a context where attribution has strategic consequences, the ability to operate discreetly becomes a defining factor.

This helps explain why many current campaigns prioritize silent access over visible exploitation. The objective is not only to gain entry, but to remain.

In this sense, technique ceases to be an end in itself and becomes a means that serves a broader strategy. The choice of tools, vectors, and targets is based on a logic that goes beyond the purely technical.

An increasingly complex ecosystem of actors

The current environment is also characterized by growing connections between state and non state actors.

Collaboration among hacktivist groups, cybercrime networks, and state linked structures creates a more adaptable ecosystem in which capabilities are shared and motives become blurred. This model not only complicates attribution but also allows states to maintain a degree of ambiguity about their true level of involvement.

In addition, the expansion of accessible tools, criminal services, and as a service models has lowered the barriers to entry, increasing the number of actors able to take part in these operations.

From a criminological perspective, this introduces dynamics typical of organized environments: specialization, outsourcing of functions, and constant adaptation based on risk and reward.

The role of Cyber Threat Intelligence in an environment of ambiguity

In this context, the main challenge for Cyber Threat Intelligence is not only detection, **but the interpretation of activity.**

The volume of available information continues to grow, but its value depends on the ability to contextualize it. Understanding a campaign requires analyzing not only how it is carried out, but also **why it occurs, when it takes place, and what strategic objective it serves.**

This implies a shift in the approach to analysis. Investigations can no longer be limited to identifying technical indicators or known patterns, but must integrate external variables such as the geopolitical context, the evolution of conflicts, and the interests of the actors involved.

From this perspective, Cyber Threat Intelligence is increasingly aligned with disciplines focused on behavioral and environmental analysis, where interpretation is as relevant as technical evidence. The ability to anticipate moves no longer depends solely on detection, but on **understanding the environment in which operations take place.**

Thus, cyberspace has become a direct extension of geopolitical competition. Operations are no longer isolated incidents, but part of continuous strategies where persistence, ambiguity, and indirect pressure shape the pace of conflict.

For this reason, in an environment where conflict is not always declared, the difference lies not in detecting more, but in interpreting better.

Sandra Somastre
Cyber Threat Intelligence Analyst

From access to intent: a CTI perspective when the attacker is a user

Article by Raquel Gálvez Huertas

More and more cyberattacks begin with seemingly legitimate access rather than a visible intrusion. The attacker does not need to breach systems; it is enough for the system to trust them.
This shift is not only operational, but structural. Traditional security has been built to detect unauthorized access. However, an increasing number of attacks use valid access, blurring the line between legitimate activity and malicious behavior.

In this context, Cyber Threat Intelligence faces a different challenge: it is no longer enough to identify external threats, but to understand how attackers behave once they appear to be users.

The shift in paradigm is best explained through the techniques that have recently gained prominence. All of them share a common element: the attacker does not “break” the system, but uses it.

When access is no longer a sign of legitimacy

One of the most representative examples is **Adversary in the Middle** phishing, which has established itself as one of the main vectors in targeted campaigns. Unlike traditional phishing, this approach makes it possible to intercept user credentials and sessions in real time, even in environments protected by multi factor authentication. The result is not only the theft of passwords, but of fully valid active sessions.

This model has reached a significant level of industrialization. In March 2026, Europol and Microsoft dismantled the **Tycoon 2FA** platform, a phishing as a service operation based on Adversary in the Middle techniques that enabled the compromise of accounts in nearly 100,000 organizations, generating large scale campaigns capable of bypassing multi factor authentication and operating with legitimate access.

This is further reinforced by the growth of **session hijacking,** especially in cloud and software as a service environments, where attackers reuse cookies or authentication tokens to access services without needing to authenticate again.

These techniques have been observed in recent incidents involving Microsoft 365 environments, where advanced actors such as **Storm 2755** accessed institutional accounts through the use of valid authentication tokens, without credentials or new login processes. Access was carried out through already issued legitimate sessions, which made detection more difficult due to the absence of obvious irregularities in the authentication process.

Persistence without credentials: the abuse of Oauth

Another emerging technique, especially relevant in corporate environments, is the abuse of **OAuth** applications. In these cases, the attacker persuades the user to authorize a malicious application that gains permissions over their account, such as email or files. From that point on, access is maintained without the need for additional credentials.
In March 2026, an active unattributed campaign abusing legitimate OAuth flows compromised more than 340 organizations by inducing users to enter codes on legitimate authentication pages, unknowingly granting attackers access and generating valid tokens without the need for credential theft. These practices introduce a new challenge: persistence no longer depends on compromised credentials, but on granted permissions.

Attacks without malware: operational invisibility

At the same time, the use of approaches known as **Living off the Land** has become more established, where attackers rely on legitimate tools within the environment, such as scripts, APIs, and cloud functionalities, to carry out their actions.
Recent campaigns by advanced persistent threat actors such **as APT29 and APT28**, driven by the geopolitical context, reflect these methods. Attackers infiltrate critical infrastructure systems using native tools, remaining undetected while extracting information for strategic purposes.
As a result, when activity relies on Living off the Land techniques, one of the main traditional indicators of compromise, malware, becomes secondary or may even disappear.

The outcome is an operation that is difficult to distinguish from that of a real user, fully integrated, with no obvious alerts or unexpected behavior.
If access is no longer a barrier, the next point of control becomes the user themselves.

The user as a bypass vector

Another relevant trend is the use of techniques that directly exploit the user as a mechanism for evasion.
MFA fatigue, also known as push bombing, involves overwhelming the user with authentication requests until, by mistake or fatigue, they approve one of them. At that point, the attacker gains access without having to bypass any technical controls.
At the same time, there has been an increase in attacks **targeting IT support services or help desks,** where attackers impersonate identities to request credential resets or changes to authentication factors. In this case, the vector is not technological, but procedural.
These mechanisms reflect a clear shift: the attacker's focus moves from weaknesses in systems to processes and people.
This approach has been repeatedly used by groups such as Scattered Spider, which in active campaigns during 2025 and 2026 have combined mass MFA notification attacks with social engineering against IT support services to obtain legitimate access in corporate environments.

Once inside, the objective is no longer to hide, but to operate without raising suspicion.

Implications for Cyber Threat Intelligence: when trust creates uncertainty

All these techniques, although different in execution, share a clear pattern: they operate within the boundaries of what the system considers normal.

- Valid access
- Legitimate tools
- Authorized processes
- Credible behavior

The integration of these factors as part of the attack itself not only reduces technical visibility, but also changes the nature of the problem that security teams face.
When there is no malware, no obvious exploitation, and no suspicious events, traditional mechanisms lose their ability to interpret what is happening.
The game is no longer about evading controls, but about fitting into them.
In this way, the value of CTI teams is no longer limited to detecting obvious signals, but evolves toward interpreting what happens within this apparent normality. Identifying patterns of use that do not fit, correlating small anomalies, and understanding attacker techniques make it possible to give meaning to activities that, in isolation, appear normal.

In an environment where access is no longer a reliable indicator, the ability to interpret behavior becomes the key element in reducing uncertainty and supporting decision making.

Raquel Gálvez Huertas
Cyber Threat Intelligence Analyst

The New Threat Landscape: Trends Redefining Our Roadmap

Trends by Alberto Herrera García

The first four months of 2026 have confirmed what we already suspected: the threat has not only grown in volume, it has changed in nature. Identity has displaced the perimeter as the main battleground, the supply chain has become a structural vulnerability, and AI is no longer an exclusive advantage of the defender but a campaign companion of the adversary. Added to this is a geopolitical landscape that defines objectives with greater precision than ever, along with a growing expectation that the analyst moves from reporting to decision making.

These are the trends redefining our roadmap.

Identity as the New Battleground Perimeter

The most compelling conclusion emerging from the main intelligence reports published so far this year is also the most uncomfortable to accept: identity has become the primary entry point into modern enterprise environments. As organizations expand into cloud platforms, software as a service ecosystems, and remote access models, traditional network boundaries have blurred. Identity now defines access, exposure, and compromise.

As a result, threat actors have adapted their operations accordingly and have widely shifted toward leveraging valid credentials obtained through infostealer malware, logs, and illicit marketplaces to log in rather than force entry and exploit systems. What the community already refers to as “log in, don’t break in.”

During 2025, hundreds of thousands of credentials for AI platforms appeared on underground markets, confirming that corporate productivity tools have become a top tier exposure vector. For operational Cyber Threat Intelligence, this trend has required redefining what exposure monitoring entails: from tracking the dark web to identifying tokens, API keys, and active sessions.

The Supply Chain: from Attack Vector to Systemic Condition

The days when supply chain attacks were isolated incidents carried out by sophisticated actors are over. Over the past five years, third party compromises have quadrupled and what was once a distinct attack category has become a permanent condition of the ecosystem. Adversaries no longer target the endpoint of the organization, but instead attack the environments where its software is built and deployed.

A clear upward trend, driven by the fragility of dependency chains, is the exploitation of public applications. A single compromised repository can distribute malicious updates to thousands of related projects before any detection system generates its first alert. For our discipline, this implies a necessary expansion of the collection model: useful intelligence must include visibility into the security posture of our suppliers, their open source dependencies, and the access they have to our infrastructure. An enriched supply chain risk map, supported by threat telemetry, is no longer a maturity aspiration, but the minimum required standard.

Adversarial AI: from tool to campaign companion

The use of artificial intelligence by adversaries is no longer a near future scenario. Malware families such as Promptflux and Promptsteal actively query language models during execution to adapt their behavior and evade detection in real time. We are facing malware capable of reasoning about its environment. At the same time, so called distillation attacks have gained relevance, allowing the extraction of proprietary logic from high value models and turning organizational AI assets into exfiltration targets as critical as any database.

The increase in attacks carried out by adversaries with AI enabled capabilities confirms that this is no longer limited to elite actors. In particular, social engineering has undergone a qualitative transformation: deepfakes generated with contextual precision, impersonation of technical support services, and multi stage phishing campaigns capable of neutralizing the human factor before the target even identifies the threat.

Geopolitics as a Strategic Intelligence Variable

No analysis of the 2026 landscape would be complete without recognizing the weight of geopolitics as a primary variable. Active conflicts, trade disputes, and the redefinition of alliances continue to shape the objectives and tempo of threat actors as decisively as any technical vulnerability. For this reason, the line that once separated financially motivated cybercrime from state sponsored espionage operations has blurred to the point where clean attribution is nearly impossible in many scenarios. Ransomware groups, for example, are simultaneously serving as sources of funding and as agents of geopolitical disruption.

At the same time, the convergence of shared tools, affiliate programs, and overlapping infrastructure has created a dynamic adversarial ecosystem in which traditional attribution models based on tactics, techniques, and procedures or on specific actors are no longer sufficient. From a strategic perspective, this situation requires analysts to incorporate geopolitics as a permanent layer of the intelligence cycle and as a predictive variable, seeking to anticipate who the next target will be, when, and with what intensity.

Intelligence as decision, not data

This overview of the main trends of the first five months of the year leaves us with a conclusion that does not require further data to support it: the complexity of the current environment cannot be addressed simply with more tools or more feeds.

It is addressed through better analytical judgment, through structures that allow intelligence to flow into action, and through the ability to maintain a strategic perspective precisely when operational noise is at its peak.

When threats move at machine speed, a defense focused exclusively on humans is no longer enough. But defensive autonomy does not imply the irrelevance of the analyst; it implies their elevation. Someone still has to design the models, calibrate the thresholds, and interpret the anomalies that no system has seen before. That role cannot be delegated. What these trends confirm is that intelligence has completed its transition from a specialized technical discipline to a top level strategic function. We have moved from collecting indicators to modeling adversaries, from monitoring threats to managing exposures, and from reporting to becoming an active part of the decision making cycle. It is a greater responsibility, but also a recognition that in an environment where adversaries operate with algorithmic speed and industrial efficiency, the only response we have is intelligence: built with rigor and applied with the judgment that only the human analyst can provide.

Alberto Herrera García
Junior Cyber Threat Intelligence Analyst

Vulnerabilities

Bypass Vulnerability in Cisco Products

Date: April 1, 2026
CVE: CVE-2026-20093

CVSS: 9.8

CRITICAL

Description

A critical authentication bypass vulnerability has been identified in the Cisco Integrated Management Controller.

This vulnerability is present in the Cisco IMC password change function, where an attacker can send a specially crafted HTTP request to a vulnerable device.

Successful exploitation could allow the attacker to bypass the authentication process, modify the passwords of any existing user, and gain access to the system as that user.

Cisco has released updates that address this vulnerability, and no alternative mitigations are currently known.

Solution

Recommendation:

- Install the appropriate update corresponding to patch level 2026 04 01 or later, depending on the affected product.

Affected Products

Some of the affected products include:

- 5000 Series Enterprise Network Compute Systems (ENCS) (CSCwq55648)
- Catalyst 8300 Series Edge uCPE (CSCwq68912)
- UCS C-Series M5 and M6 Rack Servers in standalone mode (CSCwq55659)
- UCS E-Series Servers M3 (CSCwq55648)

References

- sec.cloudapps.cisco.com
- socradar.io
- thehackernews.com

TLP:WHITE

Vulnerabilities

Docker Vulnerability Allows Unauthorized Access

Date: March 30, 2026
CVE: CVE-2026-34040

CVSS: 8.8

HIGH

Description

A high severity vulnerability has been discovered in Docker Engine that allows attackers to bypass authorization plugins and gain access to the host.

The issue is due to an incomplete fix for a previous vulnerability, which makes it possible to send crafted API requests whose content is not properly inspected by control mechanisms. As a result, privileged containers can be created with access to the host system, exposing credentials and SSH keys.

The vulnerability has been fixed in version 29.3.1, and it is recommended to update immediately or apply mitigation measures such as restricting access to the API.

Solution

- The vulnerability was fixed in Docker Engine version 29.3.1.
- It is recommended to update to this version as soon as possible.

Affected Products

- Products using Docker Engine versions earlier than 29.3.1 and that also make use of authorization plugins.
- Examples include Docker Desktop for Windows and macOS, Docker Community Edition, Docker Enterprise Edition or Mirantis Container Runtime, and Linux servers with Docker Engine installed manually.

References

- thehackernews.com
- cybersecuritynews.com

Urgent Update for Critical Vulnerability in FortiClient EMS

Date: April 5, 2026
CVE: CVE-2026-35616

Critical

Description

Fortinet has released an emergency patch for a critical vulnerability in FortiClient EMS (CVE 2026 35616), which is already being actively exploited.

The issue is due to an access control weakness that allows attackers to bypass API authentication and execute code or commands through crafted requests.

It affects versions 7.4.5 and 7.4.6, for which hotfixes have already been released, while a permanent fix will be included in version 7.4.7.

Researchers identified its exploitation as a zero day prior to disclosure and found more than 2,000 instances exposed to the internet.

Affected Products

- The vulnerability affects FortiClient EMS versions 7.4.5 and 7.4.6.
- It will also be addressed in the upcoming version 7.4.7.
- Version 7.2 is not affected.

Solution

- It is recommended to apply the patches immediately to prevent compromise.
- Patch installation links:
  - FortiClient 7.4.5
  - FortiClient 7.4.6

References

- bleepingcomputer.com
- thehackernews.com

Google Fixes a Zero Day Vulnerability

Date: April 1, 2026
CVE: CVE-2026-5281

High

Description

Google has released an urgent security patch for Chrome to address a zero day vulnerability.

The vendor's official description states that it is a use after free vulnerability in the open source implementation of the WebGPU standard, which is used in Chromium based browsers.

This vulnerability could allow a remote attacker who has compromised the renderer process used by these browsers to execute arbitrary code through a specially crafted HTML page.

The vulnerability was reported through a bug bounty program, which had previously disclosed two other vulnerabilities that were fixed in a Chrome update released on March 23.

Affected Products

Affected products include all versions of Google Chrome prior to:

- 146.0.7680.177 or 146.0.7680.178 for Windows and Mac
- 146.0.7680.177 for Linux

Solution

Recommendation:

- Update to the latest software versions.

References

- helpnetsecurity.com/
- app.opencve.io

Events

International Conference on Data Privacy and Protection, ICDPP
May 2

ICDPP brings together researchers, practitioners, and compliance professionals to address current challenges in privacy and data protection. With a strong focus on the European regulatory framework, including GDPR, the conference offers a comprehensive perspective that connects academic research with its application in enterprise environments. It is a key forum for analyzing trends in data governance, digital ethics, and regulatory compliance in a context where responsible information management is increasingly critical.

Link

CyberWiseCon Europe 2026
May 19 to 22

CyberWiseCon is a leading cybersecurity conference that brings together cybersecurity experts, industry leaders, and IT professionals from across Europe.
In a constantly evolving digital environment, knowledge alone is not enough to stay protected against cyber threats. Wisdom, gained through experience and collective understanding, enables us to stay one step ahead of malicious actors.
At CyberWiseCon, we celebrate the combination of knowledge and wisdom, providing a platform to exchange ideas, share best practices, and explore innovative approaches to cybersecurity.

Link

Cybersec Europe
20 - 21 de mayo

Cybersec Europe has established itself as one of the leading cybersecurity meeting points in Europe, bringing together experts, technology companies, and business leaders to address the most pressing challenges in the sector. The 2026 edition will focus on areas such as cloud security, identity and access management, and digital resilience, combining technological innovation with a clear strategic perspective. With a strong presence of partners and market leaders, the event also stands out for its ability to foster high level networking and collaboration opportunities.

Link

CYSAT Europe 2026
20 - 21 de mayo

CYSAT Europe represents one of the most innovative proposals in the current landscape, focused on cybersecurity applied to the space and satellite domain. In a context where critical infrastructures extend beyond the terrestrial environment, this event addresses emerging risks in space communications, satellites, and related systems. With an approach that combines industry, defense, and technology, CYSAT highlights the need to anticipate increasingly sophisticated threats in a rapidly expanding strategic domain.

Link

Resources

➢ Cyber Threat Monitor & Sector Reports

Cyble published new sector reports in April 2026, including the Healthcare Threat Landscape Report 2026, which analyzes real active threats in critical sectors. These reports provide directly actionable intelligence on ransomware, dark web activity, and targeted campaigns. They are especially useful for understanding how attackers are adapting their tactics by industry in near real time.

Link

➢ Weekly Vulnerability Digest – CVE Watchtower

This weekly briefing is highly valuable for security teams: in one recent week alone, more than 1,300 new vulnerabilities were recorded, including critical zero day issues that require immediate action. The report cuts through the noise and prioritizes what is actually exploitable, helping SOC and vulnerability management teams make fast, risk based decisions.

Link

➢ Vulnerability Statistics 2026

An extremely up to date resource: as of April 2026, more than 17,000 vulnerabilities have already been published, representing a 26% increase compared to the previous year. This dashboard, updated daily, makes it possible to understand the real pace of risk and to gauge the operational challenge faced by cybersecurity teams.

Link

Subscribe to RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com