KDDI Europe

Global Threat Intelligence Report

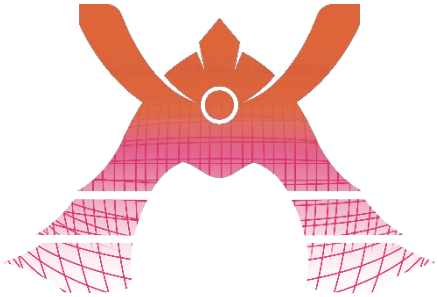
Featuring Regulatory Insights

Volume 7

November 2025

Table Of Contents

Introduction



Welcome to the Threat Report. The purpose of this document is to provide an overview of the latest cybersecurity threats, trends and regulations that could impact organisations worldwide. By analysing recent incidents and emerging threats, we aim to equip our team and customers with the knowledge and insights necessary to proactively defend against potential attacks.

At KDDI Europe, our dedication to protecting our clients and their systems is unwavering. We are continuously investing in security technologies and training our staff to enhance defences and respond swiftly to any threats. We are deeply committed to ensuring that our customers are protected in accordance with the highest standards of cybersecurity.

It is our belief that our success is linked to the success of our customers' businesses. By safeguarding your operations, we aim to provide a secure environment where your business can thrive and grow. Thank you for taking the time to review this report.

News

The Latest Cybersecurity news

Asahi Group Cyber Incident[1]

On the 29th of September 2025 Asahi Group Holdings announced that its services were disrupted to a cybersecurity incident. The beverage manufacturer stated that they were targeted by a ransomware attack but is currently withholding further details to prevent further damage. The attack affected the company's ability to accept orders and ship products and forced them to use a manual process involving pen and paper to continue some of their business activities.

Microsoft Makes Changes to Internet Explorer [2]

Although Microsoft's Internet Explorer stopped being supported in 2022, it is still used by individuals who have a need to access some websites and web applications which rely on ActiveX and Flash. IE Mode can be enabled in the Edge browser for when this need arises, however threat actors are taking advantage of this and have recently exploited Internet Explorers JavaScript engine to gain access to victims' devices. Microsoft is therefore taking action to restrain IE Mode Access. Users will still be able to use it but with a few constraints which are intended to improve security.

Threat Insights

Cyber-attacks don't just result in damage to the target, they can completely reshape competitive dynamics, create short or long-term opportunities for rivals and shift customer loyalty. Damage can be long lasting or permanent. Customers may opt for a competitor and decide to stick with them. Although a business's electronic systems may recover from an attack their customer base can be impacted beyond repair.

For example, following the cyberattack on M&S in April of 2025, one of their competitors saw an unexpected increase in sales by about 10%[3] while they (M&S) are projected to lose around £300m in profits. The claim can therefore be made that the cost of suffering an attack is always likely to exceed the cost of the tools and services that provide protection against cyber threats.

Cost will always be a major factor when making decisions around cybersecurity, so it is important that the individuals who hold the power to make such decisions are provided with as much information as possible to rationalise the choices they make.

Cybersecurity is mostly seen as an issue for technical staff, but business leaders also have a significant role to play towards building the cyber resilience of their organisation. Senior management make a bigger impact by investing in security, aligning cybersecurity with business goals, leveraging trusted MSSPs where expertise is limited or absent, and equipping technical teams with the resource needed to strengthen defences where possible. These steps improve threat detection and enable rapid response.

Cybersecurity is collaborative by nature, and it cannot be stressed how dangerous a lack of collaboration can be. Threat actors win when the parties involved in security are unable to work together properly so everyone from the Board room to the reception desk must contribute, no matter how minimal of a role they believe they play.

Regulatory Insights

EU Data Act: Enhancing Data Access, Interoperability and Portability

The EU Data Act, whose main obligations became applicable on 12 September 2025, marks a transformative shift in how Internet of Thing (IoT) data is accessed, shared, and governed across the EU. The Act empowers users - both individuals and organisations - with rights to access data they generate by using connected devices and related services [4][5]. Its aim is to democratise access and foster innovation and portability by reducing lock-in practices of manufacturers and cloud service providers.

Note that although the UK is no longer in the EU, the EU Data Act has a clear extraterritorial reach, much like the GDPR. In other words, if a non-EU company sells connected products and/or provides digital or cloud services in the EU market, it must comply with the rules of the EU Data Act. Having mentioned the GDPR, a first question comes to mind:

What are the main differences with the GDPR?

While this latter protects personal data, and constraints its use, the EU Data Act governs personal and non-personal data generated by connected devices and cloud services. As for the GDPR, compliance obligations vary depending on the role of the entity in scope: the GDPR sets out different rules for data controllers and processors [6], while the EU Data Act, introduces a wider range of roles with a variety of rights and duties. These are data holder, data user, data recipient, public authorities, manufacturers of connected products and providers of related services [7]. Another difference is that the GDPR requires controllers to have a lawful basis for processing, for example consent by the data subject, and to respect data subjects' rights and freedoms while the Data Act creates "statutory" rights for users to access and request sharing of device/service-generated data (including to third-parties if they want); where personal data are involved, GDPR's lawful-bases and safeguards continue to apply alongside the Data Act's sharing obligations. "Statutory" means that the entitlement is set forth in the Regulation and must be respected regardless of private agreements between the parties involved in the processing. In summary,

under the GDPR, emphasis falls on lawful bases, data subject rights and privacy by design. Under the Data Act, depending on their role, organisations must build secure, auditable export and delegation interfaces, ensure interoperability, support cloud-switching, and implement governance to reconcile sharing obligations with privacy duties [8].

GDPR is much about data subjects' rights. What are the user's rights under the EU Data Act?

Users have access and sharing rights for data generated by their connected products and related services. For example, they have the right to access data generated by smart home devices, wearables, connected vehicles, smart meters, industrial machinery, gaming platforms, smart TV and more, plus their related services, such as the manufacturer or third-party apps that allow to monitor and tune these devices. Manufacturers and service providers which collect the data must make it available to the user or a third-party delegated by the user in a standard format. By obtaining their data, users can switch service provider without losing their previous product usage history, get repairs from independent technicians, or even build new apps, products and services, provided that the IoT data shared by the manufacturer or service provider is not used to create a competitive product [9].

Considering that the volume of data annually generated by IoT devices is growing exponentially, potentially reaching tens of Zettabytes (1 ZB = 1 trillion gigabytes ~ streaming HD videos nonstop for 36 million years) by 2030 [10], the opportunities to spawn innovative solutions from all this data appear to be countless: from increasing operational efficiency (e.g. using sensor in machines to detect wear and tear so to replace parts before systems break down, or to start the machine when energy cost is lower), to improving Customer Experience, to data monetarisation via reselling data after appropriate aggregation and anonymisation, to building and training AI models.

Limitations apply: the Act does not entitle users or third-parties to access data generated by other people's products unless they are authorised by contract. For example, they have no blanket right to use connected product

data for training AI models. They must either be the lawful user of the product or obtain explicit consent or a licence from the lawful user or data holder. In all cases, GDPR and/or EU AI Act apply if personal data or high-risk AI is involved.

Also, if the data holder (e.g. the manufacturer of the connected product) or the user reasonably believes that sharing the data may result in severe adverse consequences for health, safety or cybersecurity, sharing will be limited. Note that the security and safety exceptions cannot be used as an excuse to avoid sharing IoT data: they only apply if EU or national law explicitly lays down security requirements for the specific industry or sector [9].

What are in-scope organisations doing to comply with the EU Data Act?

The EU Data Act entered into force on 11 January 2024 giving organisations a 20-month transition period to comply [11]. In addition, as for any EU Regulation, the legislative process was open and transparent, and drafts were circulated and debated since 2022. By mid-2023 many organisations had already started gap analyses, defined compliance roadmaps and redesigned data governance models to comply with the new rules. Organisations had to amend contracts and implement the infrastructure to make data accessible. This included adopting well documented APIs and portable industry-based standards. Enabling data sharing goes hand-in-hand with securing the interfaces and the data transport communication links, using protocols such as mutual TLS, OAuth2/OIDC for authorisation, key management and comprehensive logging for accountability [12].

In summary, the EU Data Act creates new security responsibilities for IT Security because it mandates broader access and sharing of IoT data such as smart devices metrics and related applications data. This increases the attack surface and therefore requires stronger governance, measures and monitoring. Cybersecurity controls like strong authentication, encryption of data in transit and at rest, access logging, recipient vetting, rate-limits and anomaly detection are essential to securely support Data Act rights while protecting personal data in compliance with the GDPR.

Suggestions

Protection, Prevention and Takeaways

1. Take this as a quick reminder to “think before you click”. A good rule to follow is, if you are not expecting something then it should immediately always be treated as suspicious. However, if you are expecting something, then confirm it is who you are expecting it from, briefly check the “from” address if it is a request for information or action to be taken. Having a second opinion to confirm the legitimacy of an email should be done if you are not 100% certain.

2. Threats are evolving constantly, and vulnerabilities are being discovered every day. How do you stay up to date with what is happening? Are you aware if a vulnerability has been discovered in equipment you are using? Falling behind on receiving information like this can be devastating for your business. Consider subscribing to news or RSS feeds from the vendor or provider of products and services you are using. Other sources such as threat intelligence sources (such as this) should also be considered as they can summarise information and simplify content to offer a quick read with meaningful content.

3. Cybersecurity regulations exist to protect individuals, businesses and critical infrastructure from the growing number of cyberthreats today. They can help reduce risk, make organisations legally accountable and protect sensitive data. They can also lead to stronger relationships with customers by making them feel safe when sharing their personal data. Every organisation should stay up to date with the latest cybersecurity regulations because non-compliance can lead to fines, reputational damage and legal issues.

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This report will also include the EUVD ID as well. This month it is a vulnerability affecting Windows Server.

CVE-2025-59287 | EUVD-2025-34268 [13]

Vendor	Microsoft
Product	Windows Server 2012, 2016, 2019, 2022, and 2025
Publish Date	14 Oct 2025
Platform	Windows
CVSS (v3.1)	9.8

Description

Deserialization (process of converting data from a stored or transmitted format like a file, stream, or network message back into a usable object or data structure) of untrusted data in Windows Server Update Service (WSUS) allows an unauthorized attacker to execute code over a network.

What does this mean for you?

An attacker can send an event that triggers the deserialisation of an unsafe object which will result in a remote code being executed.

What should you do about it?

Install the out-of-band update released on October 23, 2025 or for users enrolled into the hotpatch, the out-of-band standalone security update released on October 24, 2025 should be installed.

Links & References

1. Asahi Group Holdings, Ltd. (2025). Update on System Disruption Due to Cyberattack (2nd) | Newsroom | ASAHI GROUP HOLDINGS. [online] Available at: https://www.asahigroup-holdings.com/en/newsroom/detail/20251003-0204.html (Accessed: 30 October 2025).
2. Evans, G. (2025). Securing the Future: Changes to Internet Explorer Mode in Microsoft Edge. [online] Microsoft Browser Vulnerability Research. Available at: https://microsoftedge.github.io/edgevr/posts/Changes-to-Internet-Explorer-Mode-in-Microsoft-Edge (Accessed 27 October 2025).
3. Edwards, C. (2025). Next continues to profit after M&S cyber-attack. BBC News. [online] 29 Oct. Available at: https://www.bbc.co.uk/news/articles/cn0g28wgjzlo (Accessed: 29 October 2025).
4. European Commission (2025) *Today the EU Data Act starts to apply in the EU, giving users control over data generated by their connected devices, like smartwatches and cars, while unlocking opportunities for small businesses to use this data to develop innovative after-sale services.* [Press release] European Commission, 12 January. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2078 (Accessed: 31 October 2025).
5. European Parliament and Council (2023) Regulation (EU) 2023/2854 of the European Parliament and of the Council (EU Data Act). Official Journal L 2023/2854, 22 December 2023. Available at: https://eur-lex.europa.eu/eli/reg/2023/2854/oj (Accessed: 28 October 2025).
6. Information Commissioner's Office (2025) Information Commissioner's Office. Available at: https://ico.org.uk (Accessed: 28 October 2025).
7. Sircar, T. and Hodea, A. (2025) 'EU Data Act is here', National Law Review, 23 September 2025. Available at: https://natlawreview.com/article/eu-data-act-here (Accessed: 28 October 2025).
8. European Commission (2022) *Data Governance Act and Data Act*. Presentation delivered by Federico Milani, Data Policy and Innovation Unit. Slide 4: Interaction with other instruments. Available at: https://reform-support.ec.europa.eu/document/download/c632f921-91a7-4c3f-adde-32c8f4d48cdc_en?filename=Session%201%20-%20Data%20Governance%20Act%20and%20Data%20Act.pdf (Accessed: 31 October 2025).
9. European Commission (2025) *Data Act explained – Limitations on the use of the data*. Shaping Europe's Digital Future. Available at: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained (Accessed: 31 October 2025).

10. Statista (2023) Amount of data created, consumed, and stored 2010–2025. Available at: https://www.statista.com/statistics/871513/worldwide-data-created/ (Accessed: 29 October 2025).
11. European Commission (2024) *Data Act enters into force: what it means for you*. European Commission, 11 January. Available at: https://commission.europa.eu/news-and-media/news/data-act-enters-force-what-it-means-you-2024-01-11_en (Accessed: 31 October 2025).
12. Chandramouli, R. and Butcher, Z. (2025) Guidelines for API Protection for Cloud-Native Systems. NIST Special Publication 800-228. National Institute of Standards and Technology, Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.SP.800-228 (Accessed: 31 October 2025).
13. Microsoft.com. (2025). *Security Update Guide - Microsoft Security Response Center*. [online] Available at: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287 (Accessed: 30 October 2025).

Let’s Secure the Future — Together

KDDI Europe is the European headquarters of the Fortune Global 500 KDDI Corporation, delivering cutting-edge ICT and cybersecurity solutions with the precision and reliability Japan is known for.

With over 70 years of global expertise, we empower businesses across industries — from finance and retail to manufacturing and education — with secure, scalable infrastructure and 24/7 protection.

Whether you’re looking to strengthen your cybersecurity posture or scale your global operations, **we are your partner, your enabler, your platformer.**

Security of Tomorrow, Today.

Contact Information

Telephone Number	+44 20 7507 0001
Email Address	info@uk.kddi.eu

Website

LinkedIn

Enquiry