FUJITSU

November 2025

Dead Drop
Resolvers

OWASP
Top 10 2025 (release candidate 1)

The WSUS vulnerability
and why our boss jumped off the Auckland Sky Tower

Threat Intelligence Report

A monthly digest of cyber threat activities, insights, and strategies for enhanced cyber resilience

Fujitsu Cyber

Contents

This threat intelligence report has been developed using the insights from the various teams within Fujitsu Cyber. We report on the overarching trends we have recognised in the past few months, with a focus on current events and actionable steps.

At Fujitsu Cyber, we actively take these insights from what we observed and apply them to all the work we do, whether it be with our consulting engagements, our ongoing threat hunting programme, or our managed service client environments.

Our constant learning across the business helps us to stay adaptable and on top of our security game, so that we can keep your systems as safe as possible.

Dead Drop Resolvers

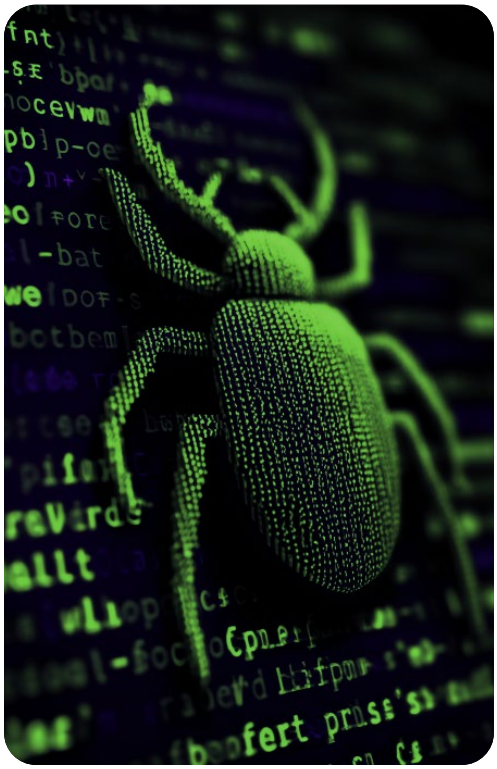
This article was written by:
Thomas Hacker
Cyber Security and Threat Intelligence Analyst

Whilst researching a new variant of the Vidar Infostealer coined 'Vidar 2.0', a stage that stood out to me was the connection between the executable and the C2 domain itself. Before reaching out to the C2 domain the malware would first attempt to reach out to a Telegram profile, and if that was not successful it would then attempt to reach out to a Steam profile. These intermediary sites were used in order to fetch the address of the C2. Whilst this is not new or specific to Vidar 2.0, this technique is known as "Dead Drop Resolver" [T1102.001]

What is a Dead Drop?

The name dead drop comes from the espionage term where spies would leave messages at an arranged secret spot for it to be later collected by another person, ensuring that they weren't seen together.

In modern times, this method of concealment has made its way to the digital world.



Background

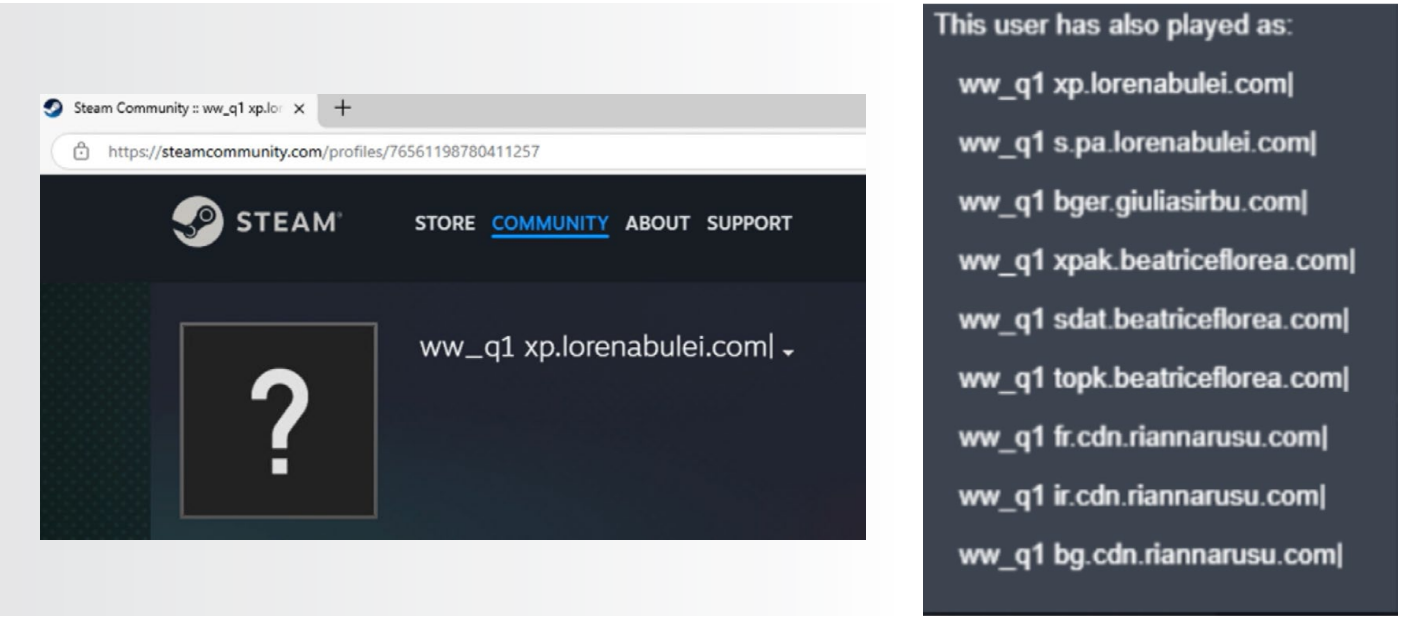
When creating malware, attackers may communicate between a C2. In doing this the malware will need to be able to know the address. There are numerous techniques to do this, however, the problem for attackers is that once the malware has been compiled, the code is unable to be edited. This means that the C2 addresses are often required to be hard coded into the malware. The majority of the time these addresses are obfuscated to make it difficult for defenders to combat it.

However, using dynamic analysis techniques and watching the network flow, it's often easy to see where this malware points to.

Once the malware is deployed and being distributed to unknowing victims, if the malware points to one single C2 domain it's very easy for the cloud hosting providers to perform a take down. This is because it will likely violate T&C's due to it being used for malicious purposes. Alternatively, defenders can simply apply a block to the address that the malware is being hosted.

This is where the technique "Dead Drop Resolver" comes into play.

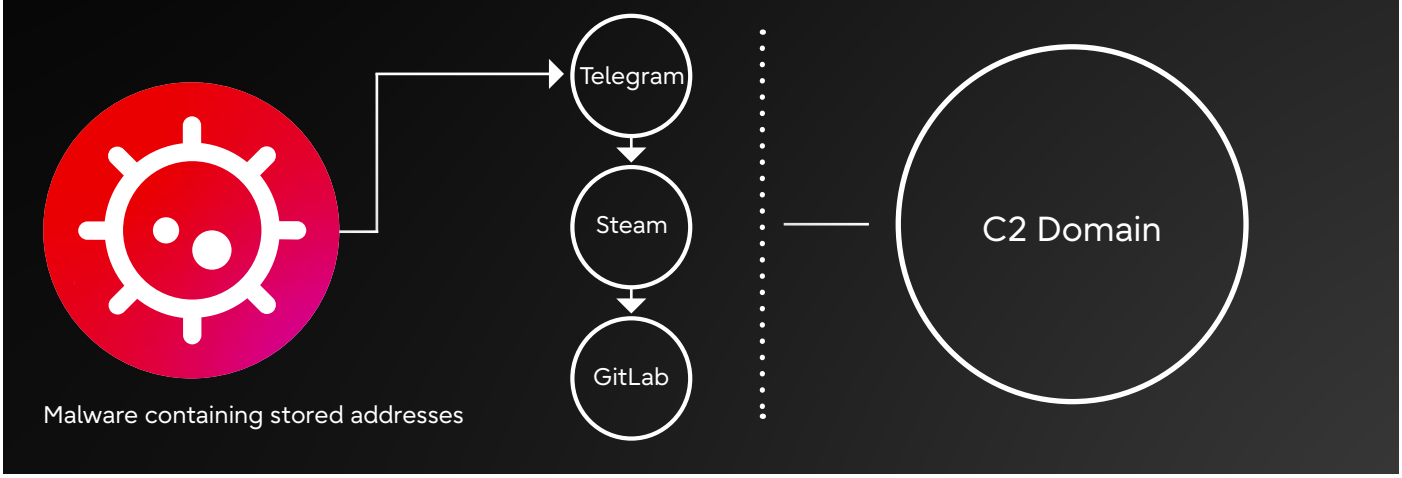
Adding an additional hop within the network flow allows the attackers to dynamically change the address of the C2 when required. For example, see the below steam profile:



As you can see the profile name for this account is pointing to a domain where the C2 is located. When you hover over previous names you can see how it's been changed numerous times, indicating that the C2 has been rotated to different addresses.

This allows the malware to have a much longer shelf life and remain more effective for longer periods of time. It also adds to the constant cat and mouse chase that attackers and defenders are constantly engaged in. As C2 IOCs are discovered and defenders are utilising these, the attacker can simply point to a new C2, putting defenders on the hunt again.

The below diagram shows a fictitious example of what the hops may look like in a DDR infostealer:



A few of the social media sites that have been observed as the trusted medium to host these addresses are but not limited to:

- Steam
- Telegram
- TikTok
- Mastodon
- IOC Exchange
- Nerdculture
- GitHub
- GitLab

How can this help defenders?

Given that there is a hop before the C2 is reached, this gives defenders the opportunity to utilise the technique "reduce attack surface", by blocking access to these "trusted" sites if they are not used within the environment. Whilst this may provide prevention against some of the attacks, there will always be a trusted site within your organisation that will be able to be leveraged. For example, take GitHub and GitLab. If your organisation does development work, it's highly likely that you are using one or the other and blocking access to this simply isn't feasible as it would disrupt day to day operations.

Another method would be through the usage of anomaly-based detections. Seeing as in this situation it's impossible to completely eradicate the risk as there will always be some form of trusted medium that attackers can utilise. **Looking into the pattern of behaviour through the lens of network monitoring tools, is critical.** Through the usage of machine learning to analyse timing and data patterns can help build analytics to detect usage of this technique.

References

[1] https://www.reversinglabs.com/blog/malware-leveraging-public-infrastructure-like-github-on-the-rise
[2] https://www.darktrace.com/blog/vidar-info-stealer-malware-distributed-via-malvertising-on-google
[3] DPRK-linked GitHub C2 Espionage Campaign
[4] https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/
[5] https://cyberpress.org/acrstealer-leverages-google-docs-and-steam/
[6] https://asec.ahnlab.com/en/89128/
[7] https://community.emergingthreats.net/t/vidar-stealer-picks-up-steam/271
[8] https://www.hhs.gov/sites/default/files/vidar-malware-analyst-note-tlpclear.pdf
[9] https://blog.bushidotoken.net/2021/04/dead-drop-resolvers-espionage-inspired.html
[10] Web Service: Dead Drop Resolver, Sub-technique T1102.001 - Enterprise | MITRE ATT&CK®

Article two:

OWASP Top 10 2025 (release candidate 1)

This article was written by:
James Nicoll
Technical Tester

On the 6th of November 2025, the first release candidate (RC) for the new OWASP Top 10 was made available.

The OWASP Top 10 is a report on the 10 most common, critical risks and vulnerabilities affecting web applications around the world. It uses data submitted by security researchers, software vendors, bug bounty programs, and a community survey to determine both what is commonly reported and what the cyber security community are reporting to have seen.

The 2025 report is in the RC phase, and the previous version (OWASP Top 10 2021) is still considered the current release version. However, the release candidate is a good indication of the data the final 2025 report is being built on. With each release, OWASP provides a table showing the changes of the current Top 10 to the previous report.

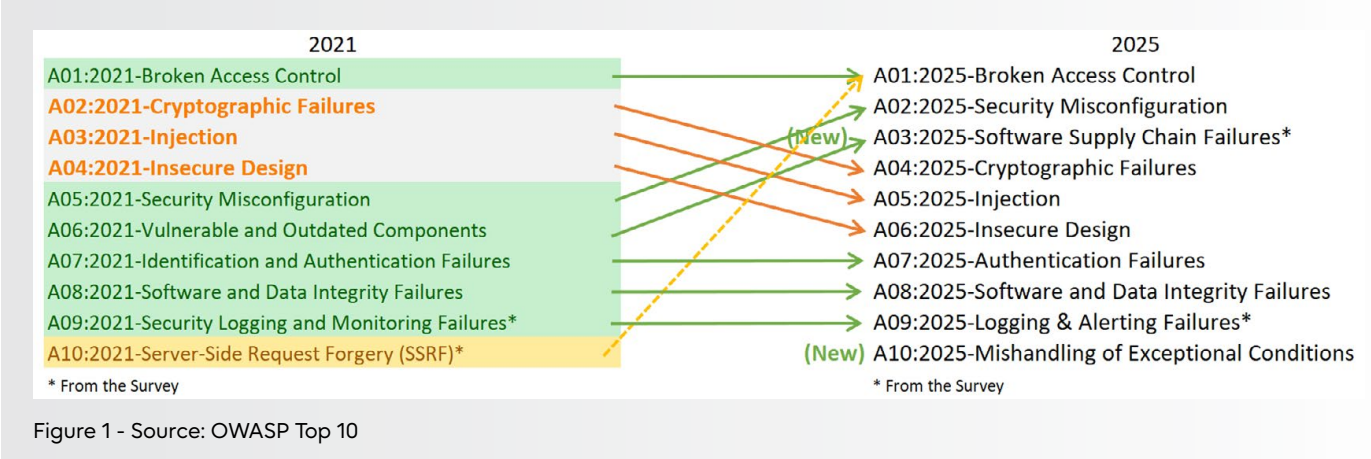
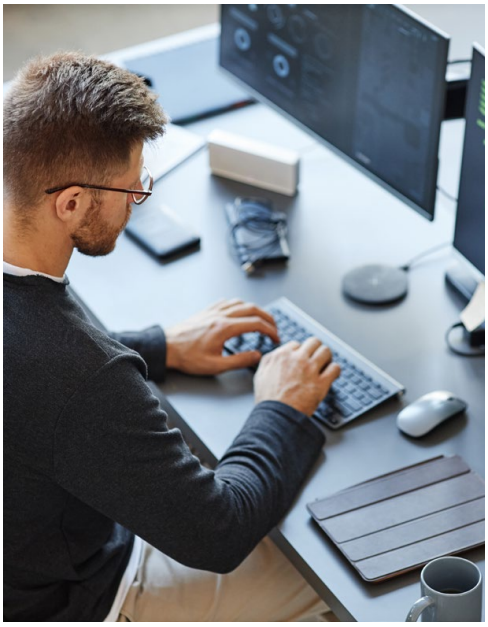


Figure 1 - Source: OWASP Top 10

As we can see in the table above, **Broken Access Control** remains the most common vulnerability found in Web Applications. For 2025, the Server-Side Request Forgery (SSRF) vulnerabilities have been bundled into A01: Broken Access Control.



Security Misconfiguration and **Vulnerable and Outdated Components** have been moved to second and third place respectively, with Vulnerable and Outdated Components being expanded to Software Supply Chain Failures. This now includes all supply chain failures, not limited to just using vulnerable components.

Cryptographic Failures, Injection, and **Insecure Design** have all dropped by 2 positions. OWASP has noted that they have seen improvements in the web development community when it comes to these vulnerabilities, leading to them being less frequent and subsequently falling lower in the Top 10 rankings.

Authentication Failures, Software and Data Integrity Failures, and Logging and Alerting Failures all remain in their previous positions with a few name changes to better reflect what the categories are representing.

Finally, a new category has been added at position 10. **Mishandling of Exceptional Conditions**. This category focuses on risks and vulnerabilities related to how errors and unexpected events or user inputs can lead to misbehaviour by the application. This could result in issues with authentication, authorisation, or data leakage. Mishandling of Exception Conditions looks at how an application deals with unexpected or situations, OWASP lists the following 3 failings as mishandling exceptional conditions:

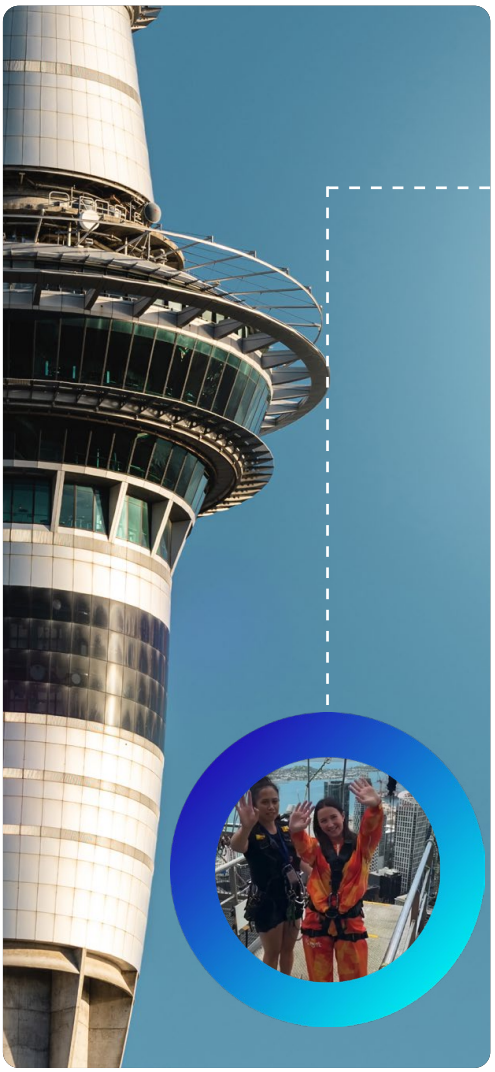
1. **The application is unable to identify unusual situations.**
2. **The application allows unusual situations to happen.**
3. **The application responds poorly to unusual situations.**

The OWASP Top 10 2025 (RC1) shows a positive industry trend towards preventing cryptographic failures, injection vulnerabilities, and insecure design. Despite this, Broken Access Control remains a frequent risk for all web applications, it is important for developers to test authentication and authorisation controls within their applications to ensure their own controls are not vulnerable to attack.

The WSUS vulnerability and why our boss jumped off the Auckland Sky Tower

This article was written by:
Hilary Bea
Senior Consultant

In Cybersecurity, success depends on preparation, having trust in your team, your systems, and knowing what risks you're willing to take.



This month, our Security Operations Practice Lead **Taylor Shera** swapped dashboards and detection rules for harnesses and heart rates, by participating in Drop Your Boss 2025, a 192-metre drop off Auckland's Sky Tower on the 27th of November, in support of the Graeme Dingle Foundation's work building resilience in young people [1].

Our young people growing up today are facing a world of increasing challenges and adversity. 60% of Kiwi kids fear failure, nearly one in four report symptoms of depression, and New Zealand has one of the highest bullying rates in the world. For 30 years, the Graeme Dingle Foundation has been standing alongside tamariki (children) and rangatahi (teenagers and young adults), helping them build confidence, resilience, and the life skills they need to thrive [2].

The act of risk-taking and preparation required for Taylor's jump provides compelling parallels to cybersecurity, and more recently, a critical vulnerability uncovered in WSUS (Windows Server Update Services). WSUS is the key patch-management backbone for many enterprises, ensuring that their systems stay patched and up to date. However, last month, that safety-line frayed. This vulnerability (CVE-2025-59287), uncovered in late October 2025, exposed how a trusted safety line (patching via WSUS) can fray, not because of negligence, but because an attacker found a way to bypass the controls [3].

Technical overview of CVE-2025-59287

This critical Remote Code Execution (RCE) vulnerability in Microsoft's WSUS service allows an unauthenticated attacker to execute arbitrary code with SYSTEM privileges on a vulnerable server [3].

The vulnerability arises from unsafe deserialisation of untrusted data. Specifically, the WSUS server role's web services accept an encrypted "AuthorizationCookie" object, which is decrypted and then passed to the .NET `BinaryFormatter.Deserialize()` method without sufficient type validation. An attacker can craft a malicious serialised object (a gadget chain) which, when deserialised, triggers arbitrary code execution [4].

There are a lot of risk implications with this. Once a WSUS server is compromised, the attacker has SYSTEM privileges on a trusted patch-infrastructure component. They could distribute malicious updates, pivot laterally, and continue further compromise across the enterprise.

Affected systems: Only servers with the WSUS Server Role enabled are vulnerable. This includes Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022 (including 23H2), and 2025-Server-Core builds, up to specific build numbers [5].

Attack surface and exploitation:

WSUS servers often expose ports TCP 8530 (HTTP) or TCP 8531 (HTTPS) for client update traffic [3].

In observed attacks, process chains like wsusservice.exe → cmd.exe → powershell.exe and w3wp.exe → cmd.exe → powershell.exe were seen [3].

Real-world exploitation has already been seen, and this vulnerability was added to the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalogue on the 24th of October 2025 [5].

Recommendations

Inventory and prioritise your assets and systems

Identify and classify all systems affected by a vulnerability so that remediation can focus first on those with the highest exposure and business impact.

Apply all security patches immediately

Deploy vendor patches as soon as they become available to minimise the window in which an exploitable weakness remains open.

Implement interim mitigations if patching is delayed

Where patching cannot occur immediately, apply compensating controls such as network restrictions, role deactivation, or configuration hardening to reduce risk.

Update monitoring, detection, and incident response playbooks

Ensure logging, detection rules, and incident response procedures are updated to recognise exploit attempts and guide swift containment actions.

Strengthen readiness and cybersecurity posture

Prepare for the possibility of exploitation by validating backups, practising restoration, and conducting threat hunting for suspicious activity.

Re-evaluate access controls and segmentation

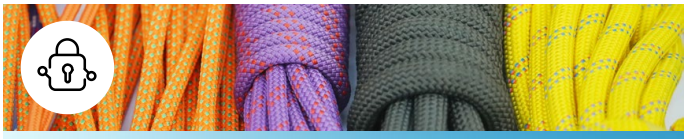
Review and tighten access pathways and network boundaries to minimise lateral movement and limit the blast radius of any potential compromise.

Parallels to "Drop Your Boss - Graeme Dingle Foundation"

Just as Taylor trusted her safety team, gear, and contingency plans to guide a safe drop and landing, our organisations must trust their patch-management infrastructure, monitoring, and fallback controls to protect against threats. The recent WSUS vulnerability reminds us that even our most trusted system can become a point of failure if it's not well-managed. Consider the following parallels:

Harness check = Patch status verification

Before stepping off the platform, each buckle and strap is inspected. In this cyber case, we must verify that WSUS servers are patched with the relevant emergency updates (e.g., KB5070882/5070883 etc.) [6].

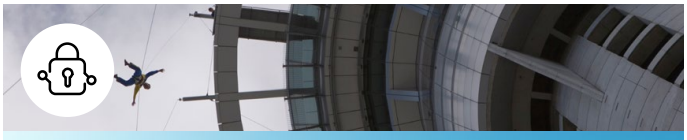


Ground team + backup ropes = Monitoring and detection rules

If the main rope fails, the reserve must kick in. Our SIEM/EDR alerts must detect anomalous behaviour that might indicate exploitation (e.g., wsusservice.exe spawning powershell.exe) [3].

Jump platform = Trusted infrastructure

WSUS has historically been a platform of trust in enterprise patch management. However, if that platform becomes the entry point for attack, the entire jump becomes jeopardised.



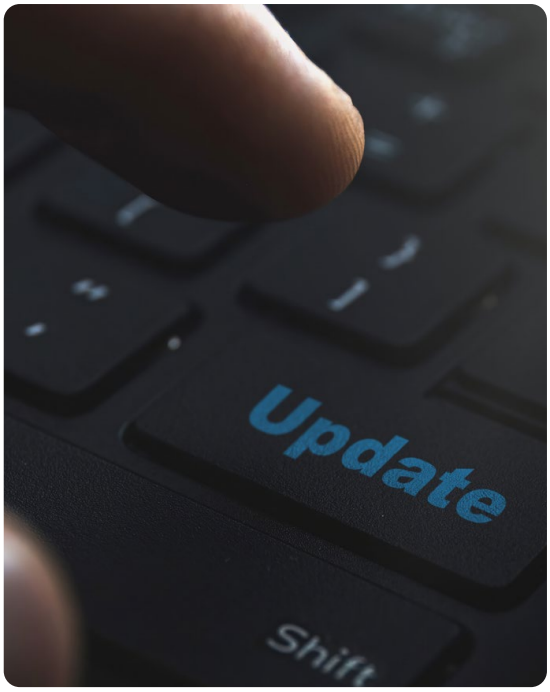
Freefall acceptance = Accepting residual risk

Jumping off 192 metres requires accepting some risk, but it's mitigated through preparation, equipment, and training. Similarly, in cybersecurity we accept that there cannot be no risk, however, we reduce it through controls, readiness, and risk assessments.

Conclusion

On the day of Taylor's drop off the Sky Tower, she relied on every piece of gear, the team coordinating her, and the backup systems in place. When a system like WSUS is compromised, that same logic applies. Our "gear" (patch mechanisms), our "team" (detection, monitoring, incident response) and our "backup ropes and systems" (controls, segmentation, fallback mitigations) must all deploy smoothly.

The discovery of CVE-2025-59287 is a stark reminder that trusted infrastructure is only as good as its latest patch and how well we test and prepare for failure. If we ensure our systems are reinforced with layered controls and validated safeguards, we can be confident that our security posture is resilient, responsive and ready for whatever threat emerges next.



Let Taylor's jump be a symbol of not only personal courage, but also of our collective commitment to risk-awareness, preparation, and resilience in cybersecurity.

References

[1] Graeme Dingle Foundation, "Drop Your Boss," [Online]. Available: https://dinglefoundation.org.nz/dyb/. [Accessed: Nov. 6, 2025].
[2] Drop Your Boss, "Taylor Shera (Fujitsu) Drop Your Boss 2025," [Online]. Available: https://dropyourboss.co.nz/taylor-shera-fujitsu. [Accessed: Nov. 6, 2025].
[3] Unit 42, "Microsoft WSUS Remote Code Execution (CVE-2025-59287) Actively Exploited in the Wild," Palo Alto Networks, Nov. 3, 2025. [Online]. Available: https://unit42.paloaltonetworks.com/microsoft-cve-2025-59287/. [Accessed: Nov. 11, 2025].
[4] Picus Security, "CVE-2025-59287 Explained: WSUS Unauthenticated RCE Vulnerability," Oct. 25, 2025. [Online]. Available: https://www.picussecurity.com/resource/blog/cve-2025-59287-explained-wsus-unauthenticated-rce-vulnerability. [Accessed: Nov. 11, 2025].
[5] National Vulnerability Database (NVD), "CVE-2025-59287," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-59287. [Accessed: Nov. 12, 2025].
[6] Microsoft Support, "October 23, 2025—KB5070882 (OS Build 14393.8524) Out-of-band," [Online]. Available: https://support.microsoft.com/en-au/topic/october-23-2025-kb5070882-os-build-14393-8524-out-of-band-3400c459-db78-48bc-ae69-f61bff15ea7c. [Accessed: Nov. 12, 2025].

Stay compliant. Remain protected.

We are a Trans-Tasman team providing end-to-end cybersecurity solutions to protect organisations in Oceania from evolving threats. We help you align with best practices, strengthen your defences, and ensure your systems are resilient and compliant.

Framework aligned

Fujitsu Cyber is **CREST-accredited** and aligns to government and industry frameworks (ISO 27001, Essential Eight, ISM/NZISM, IRAP, + more).

More than just risk reports

We don't just identify issues - we guide strategic improvements allowing you to make informed decisions about your cyber strategy.

Local trust, global strength

Trusted ANZ-based delivery backed by worldwide strength and cutting-edge innovation.

Key trends

Fujitsu Cyber draws on all parts of the business to identify key trends and changes with relevance to companies operating in New Zealand and Australia, both now and in the future. These threats may not all be completely technical, also relating to business operation, operations in New Zealand, Australia, or global events that have a bearing on New Zealand and Australia's cybersecurity environment. You may also be interested in our 'Best of 2025 Threat Intelligence Report' here

Feedback

We welcome feedback on the usefulness of this report or requests for specific focus. Please send your feedback to

Thomas.Hacker@fujitsu.com