MDR CYBER
Part of the Mishcon de Reya Group

August 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

August 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
In July, a flawed CrowdStrike update crashed thousands of global computers, significantly disrupting business operations.	The manual workaround for the software issue led to prolonged recovery, causing widespread and immediate business disruptions.	Post-incident, businesses should prioritise technical solutions, check insurance for coverage, update customers, consider regulators, and review contracts for compliance and liability.
Ransomware groups observed exploiting ESXi Hypervisor vulnerability to encrypt data.	After gaining initial access, multiple threat actors were able to easily exploit the vulnerability to access multiple machines.	ESXi is favoured by attackers due to its common usage. Users should install the updates released by VMware, as well as tighten security monitoring and perform scans to identify vulnerabilities in network devices.

Preparing decision makers

Our monthly report prepares cybersecurity practitioners to make better tactical, operational and strategic decisions. We have distilled analysis of key events from the previous month which have learning points that can be actioned to improve security.

The document has three main purposes to assist cybersecurity leaders:

1. To be 'threat-led' and help prioritise defences against particular types of attackers
2. To justify business decisions on cybersecurity changes, technology or services
3. To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

Lessons learned from the CrowdStrike outage

What happened?

From 18 July 2024, a faulty update in CrowdStrike's cyber security Falcon Sensor software[1] caused thousands of computers worldwide to crash causing massive operational impact to businesses. The outage was caused by a coding error and was not a cyber-attack. Although a workaround was quickly released, the process was largely manual, meaning that recovery in some cases took an extended time.

As the software is widely used by many businesses, the issue had severe short-term direct, and indirect supply-chain impacts for the business operations of many companies globally. The overall costs to the US Fortune 500 alone were estimated to be more than $5.4bn.[2]

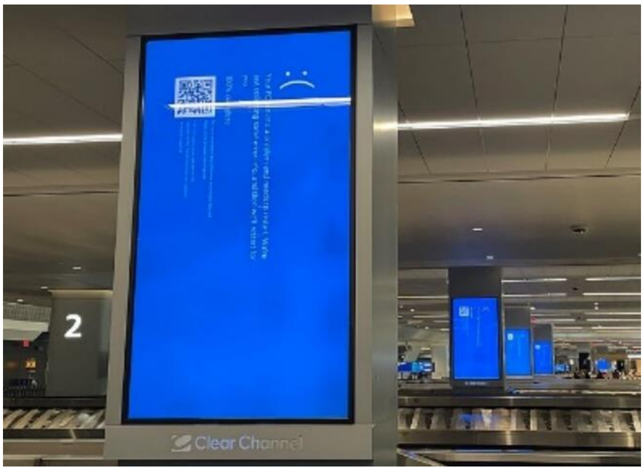


Figure 1 - "Blue Screen of Death" at LaGuardia Airport, New York (source: Wikimedia Commons[3])

So what?

Despite the rarity of such incidents, the event highlighted the risks associated with software updates and the importance of including cloud outages in business continuity planning. Having a well-prepared and defined incident response plan is critical for mitigating such issues, this should be underpinned by thorough risk assessment, which considers these kinds of issues.

Cyber security leaders are cautioned against downgrading security updates out of fear of similar occurrences. Slowing down patching may be perceived as a safer option considering this incident but given the high number of vulnerabilities disclosed, this approach is not likely to be scalable and, as the process is often a race against time, automated or phased patching is preferable.

Key steps for businesses in the aftermath should include focusing on technical fixes to mitigate losses, reviewing insurance policies, communicating with customers and stakeholders, notifying regulators if necessary, and being vigilant against potential cyber threats exploiting the situation.

[1] Remediation and Guidance Hub, https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

[2] CrowdStrike global outage to cost US Fortune 500 companies $5.4bn, https://www.theguardian.com/technology/article/2024/jul/24/crowdstrike-outage-companies-cost

[3] File:CrowdStrike BSOD at LGA.jpg, https://en.m.wikipedia.org/wiki/File:CrowdStrike_BSOD_at_LGA.jpg

Businesses are also advised to review their contractual arrangements to ensure compliance and to assess potential liability or the ability to recover losses.

Mishcon have published a briefing note covering these issues in greater detail.[4]

[4] CrowdStrike update causes global impacts, https://www.mishcon.com/news/crowdstrike-update-causes-global-impacts

Ransomware groups exploit ESXi hypervisor vulnerability to gain administrative rights

What?

On 29 July 2024, Microsoft uncovered a vulnerability in the ESXi hypervisor which was being exploited by ransomware operators to gain full administrative permissions on domain-joined ESXi hypervisors. The exploitation of this vulnerability, designated as CVE-2024-37085, allowed threat actors to encrypt the file system and target virtual machines (VMs) hosted on the affected ESXi hypervisors, potentially disrupting the functionality of hosted servers and enabling lateral movement within the network.[5] The ease of exploitation has likely led to the widespread adoption of it as a favoured technique.

An ESXi hypervisor is similar to software installed on a physical server that divides that server into multiple VMs. Each VM can run its operating system and applications as if it were a separate physical computer, even though they all share the same underlying physical hardware. In this way, it allows one computer to do the job of many.

The vulnerability could be exploited in at least three ways for domain-joined ESXi hypervisors:

1. Adding the "ESX Admins" group - if there is not already an "ESX Admins" group, someone with the rights to create groups in the network can simply set up this "ESX Admins" group themselves. They can then give themselves or others full control over the connected ESXi hypervisors by adding those users to the newly created group. It was this simple technique that has been observed "in the wild".

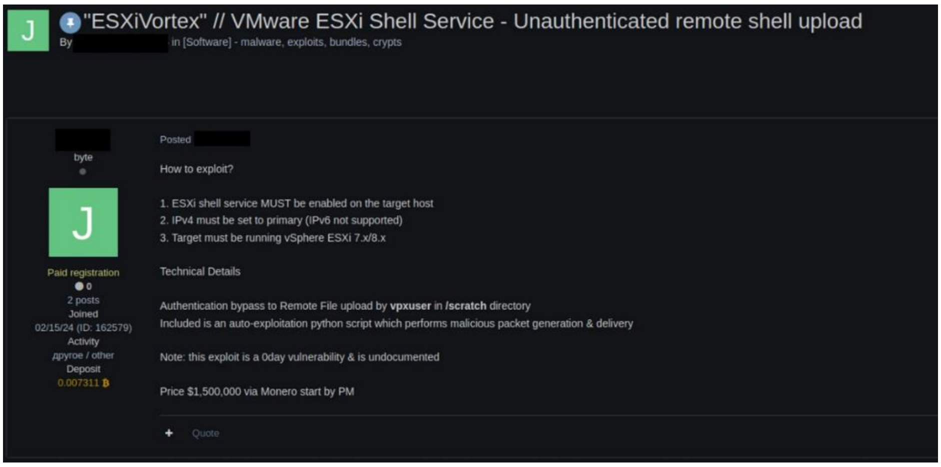
2. Renaming a group as "ESX Admins" - if an attacker has control over a user account that has the rights to change group names within the network, they can take any group and rename it to "ESX Admins". They can then either add a new user to this group or use an existing member to gain full administrative control. However, this method had not been seen used in real attacks.

3. Refreshing ESXi hypervisor privileges - If the network manager switches the control of the ESXi hypervisor to a new group, the original "ESX Admins" group keeps its full access for a while. This could be a chance for hackers to take advantage. This also had not been seen in actual attacks.[6]

Code to exploit EXSi vulnerabilities were being marketed by criminal forum users for USD 1.5m dollars, indicating its relatively high value (see Figure 2).

[5] Ransomware gangs are loving this dumb but deadly make-me-admin ESXi vulnerability, https://www.theregister.com/2024/07/30/make_me_admin_esxi_flaw/

[6] VMware ESXi CVE-2024-37085 Targeted in Ransomware Campaigns https://www.rapid7.com/blog/post/2024/07/30/vmware-esxi-cve-2024-37085-targeted-in-ransomware-campaigns/,



J "ESXiVortex" // VMware ESXi Shell Service - Unauthenticated remote shell upload

By [redacted] in [Software] - malware, exploits, bundles, crypts

[redacted]
byte

Paid registration
● 0
2 posts
Joined
02/15/24 (ID: 162579)
Activity
дpyroe / other
Deposit
0.007311 ₿

Posted [redacted]

How to exploit?

1. ESXi shell service MUST be enabled on the target host
2. IPv4 must be set to primary (IPv6 not supported)
3. Target must be running vSphere ESXi 7.x/8.x

Technical Details

Authentication bypass to Remote File upload by **vpxuser** in **/scratch** directory
Included is an auto-exploitation python script which performs malicious packet generation & delivery

Note: this exploit is a 0day vulnerability & is undocumented

Price $1,500,000 via Monero start by PM

Figure 2: ESXi unauthenticated shell for sale on the dark web, (source: Microsoft[7])

So what?

Ransomware operators have targeted ESXi hypervisors in the recent past, as it allows for mass encryption of multiple machines and maximum impact. As this software is commonplace, this makes it an appealing target for attackers and worthy of enhanced vigilance for any organisation using it.

The vulnerability was only assigned a low rating in the Common Vulnerability Scoring System (CVSS) of 6.8 as it requires prior compromise, meaning that it may not be prioritised by some security teams. However, it has been observed being used widely by threat actors and therefore worthy of attention.

To protect against the CVE-2024-37085 vulnerability, administrators of ESXi servers should apply the security updates released by VMware. In addition to patching, the following mitigation strategies are advised:

1. Validate and secure the "ESX Admins" group within the domain.
2. Manually deny access to this group by altering settings in the ESXi hypervisor.
3. Change the admin group in the ESXi hypervisor to a different, secure group.
4. Implement credential hygiene by enforcing multifactor authentication, enabling password less authentication methods, and isolating privileged accounts.
5. Improve the security posture of critical assets, such as ESXi hypervisors by ensuring they are updated, monitored, and have backup and recovery plans in place.
6. Identify vulnerable assets through authenticated scans and monitor for suspicious administrative access.

Microsoft also recommends running the following Kusto quey language (KQL) queries in Defender to find related activity in an organisation:

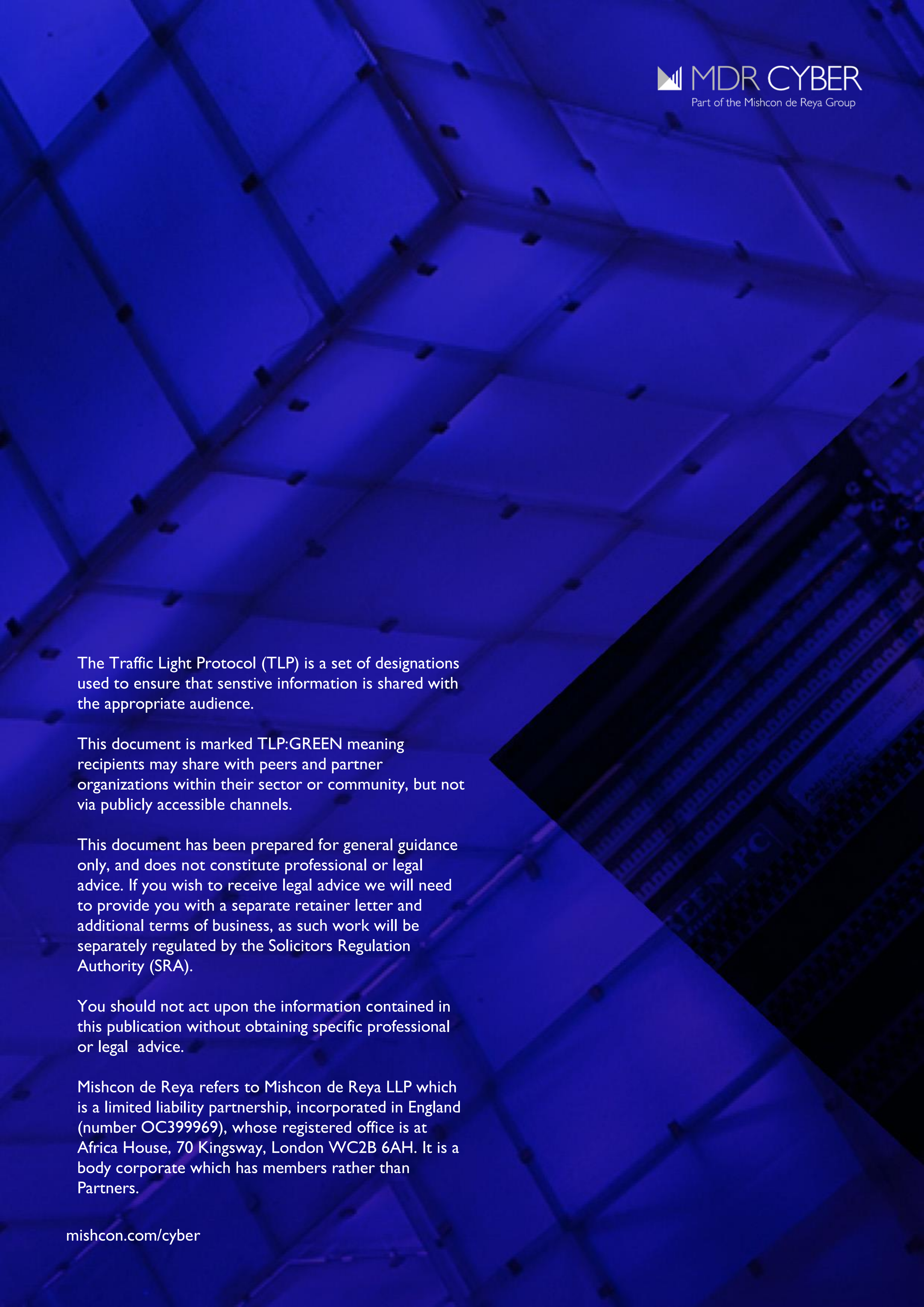
[7] Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption, https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/

This query would identify presence of ESXi hypervisor in the organisation:

```
DeviceInfo
| where OSDistribution =~ "ESXi"
| summarize arg_max(Timestamp, *) by DeviceId
```

The query below identifies ESX Admins group changes in the Active directory:

```
IdentityDirectoryEvents
| where Timestamp >= ago(30d)
| where AdditionalFields has ('esx admins')
```



MDR CYBER
Part of the Mishcon de Reya Group

The Traffic Light Protocol (TLP) is a set of designations used to ensure that senstive information is shared with the appropriate audience.

This document is marked TLP:GREEN meaning recipients may share with peers and partner organizations within their sector or community, but not via publicly accessible channels.

This document has been prepared for general guidance only, and does not constitute professional or legal advice. If you wish to receive legal advice we will need to provide you with a separate retainer letter and additional terms of business, as such work will be separately regulated by the Solicitors Regulation Authority (SRA).

You should not act upon the information contained in this publication without obtaining specific professional or legal advice.

Mishcon de Reya refers to Mishcon de Reya LLP which is a limited liability partnership, incorporated in England (number OC399969), whose registered office is at Africa House, 70 Kingsway, London WC2B 6AH. It is a body corporate which has members rather than Partners.

mishcon.com/cyber