TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 25, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

In today's rapidly evolving digital environment, proactive cybersecurity is essential for organisations across all industries. Our weekly Cyber Threat Intelligence (CTI) reports deliver crucial insights into emerging threats, vulnerabilities, and attack trends, enabling businesses to strengthen their defences and stay ahead of evolving risks.

By combining expert analysis with actionable strategies, we empower clients to anticipate, detect, and mitigate potential threats before they escalate. This proactive approach safeguards critical digital assets, ensures operational continuity, and builds stakeholder trust. With our CTI reports, organisations can develop enduring cyber resilience, fostering security and confidence in an increasingly unpredictable digital landscape.

Microsoft releases urgent patches to address 57 critical security flaws

In a critical move to safeguard users, Microsoft has rolled out urgent patches addressing 57 security vulnerabilities across its software ecosystem. The March 2025 update includes fixes for multiple high-severity flaws, some of which could allow remote code execution, privilege escalation, and data breaches if exploited. Among the most concerning is a zero-day vulnerability actively being exploited by cybercriminals, underscoring the need for immediate action. The patches impact a wide range of Microsoft products, including Windows, Office, Azure, and Edge.

Cybersecurity experts are urging organisations and individual users to apply the updates promptly to mitigate risks. Microsoft has emphasised the importance of these patches in preventing potential large-scale attacks, particularly targeting enterprises and government agencies. This update highlights the escalating threat landscape and the critical role of timely software maintenance in defending against sophisticated cyberattacks. Users are advised to enable automatic updates or manually install the patches to ensure robust protection.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://thehackernews.com/2025/03/urgent-microsoft-patches-57-security.html

TATA COMMUNICATIONS

Critical vulnerabilities in Adobe products expose users to arbitrary code execution

A recent advisory has revealed multiple high-severity vulnerabilities in Adobe products, posing significant risks to users. These flaws, identified in popular software such as Acrobat, Reader, and Photoshop, could allow attackers to execute arbitrary code, potentially leading to system compromise, data theft, or malware installation. The vulnerabilities stem from memory corruption and improper input validation issues, which cybercriminals could exploit by tricking users into opening malicious files or visiting compromised websites. Adobe has released patches to address these critical flaws, urging users to update their software immediately to mitigate risks.

With Adobe products widely used across industries, the potential impact of these vulnerabilities is substantial. Researchers emphasise the importance of proactive cybersecurity measures, including regular software updates and user vigilance, to defend against evolving threats. Organisations and individuals are advised to apply the patches promptly to safeguard their systems and data.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Adobe

Source - https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-products-could-allow-for-arbitrary-code-execution_2025-023

TATA COMMUNICATIONS

SAP issues security updates to address vulnerabilities in March 2025 patch release

SAP has released its March 2025 security updates, addressing multiple critical vulnerabilities across its software portfolio. These patches target flaws that could expose businesses to risks such as data breaches, privilege escalation, and system compromises if left unpatched. Among the highlighted issues are high-severity vulnerabilities in SAP S/4HANA, SAP Business One, and SAP NetWeaver, which could be exploited by attackers to gain unauthorised access or disrupt operations. The updates underscore SAP's commitment to proactive cybersecurity, urging customers to apply patches immediately to mitigate potential threats.

SAP has also emphasised the importance of regular system updates and monitoring to safeguard sensitive business data and maintain operational integrity. With SAP systems widely used in enterprise environments, these vulnerabilities pose significant risks to organisations globally. Cybersecurity experts recommend prioritising the installation of these patches and conducting thorough system reviews to ensure comprehensive protection against evolving cyber threats.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	SAP

Source - https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2025.html

Critical vulnerabilities discovered in Zoom, prompting urgent updates

Recent cybersecurity research has uncovered multiple high-severity vulnerabilities in Zoom, raising concerns over potential exploitation by attackers. These flaws, affecting both desktop and mobile versions, could allow unauthorised access to sensitive data, remote code execution, and even complete system compromise. Among the identified risks are improper input validation and memory corruption issues, which could be exploited through malicious meeting invites or crafted files. Zoom has swiftly released patches to address these vulnerabilities, urging users to update their software immediately.

The company emphasised the importance of staying on the latest version to mitigate risks and ensure secure communication. Cybersecurity experts have echoed this advice, warning that unpatched systems could be targeted by cybercriminals to steal sensitive information or disrupt operations. With Zoom being a critical tool for remote work and collaboration, these vulnerabilities pose significant risks to businesses and individuals alike. Users are advised to enable automatic updates or manually install the latest version to safeguard their systems.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Zoom

Source - https://cybersecuritynews.com/multiple-zoom-client-vulnerabilities/

TATA COMMUNICATIONS

Louis ransomware emerges as a growing threat that requires immediate action

A new ransomware strain, dubbed Louis, has been identified as a significant threat to individuals and businesses alike. This malicious software encrypts victims' files, demanding ransom payments in exchange for decryption keys. Louis ransomware typically infiltrates systems through phishing emails, malicious attachments, or compromised websites, exploiting vulnerabilities to gain access. Cybersecurity experts warn that paying the ransom does not guarantee file recovery and may further incentivise attackers. Instead, they recommend proactive measures such as regular data backups, robust antivirus software, and employee training to recognise phishing attempts.

For those already affected, removal tools and guides are available to help eliminate the ransomware and restore systems. However, prevention remains the best defence. Authorities urge users to update software, enable firewalls, and avoid suspicious links or downloads. As ransomware attacks continue to rise, the emergence of Louis underscores the critical need for heightened cybersecurity awareness and preparedness to combat evolving digital threats.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://www.cyclonis.com/remove-louis-ransomware/

CISA expands catalogue with six more critical vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA) has added six new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue, warning organisations to address these flaws immediately. These vulnerabilities, actively being exploited by attackers, affect widely used software and systems, posing significant risks such as remote code execution, data breaches, and system takeovers. CISA's advisory highlights the urgent need for patching and mitigation to prevent potential cyberattacks. The affected products include popular platforms used across industries, making the threat particularly widespread. Federal agencies are mandated to remediate these vulnerabilities within strict deadlines, while private sector organisations are strongly encouraged to follow suit.

This update underscores the growing sophistication of cyber threats and the importance of proactive vulnerability management. CISA urges all entities to review the KEV catalogue, apply necessary patches, and implement robust cybersecurity measures to safeguard critical infrastructure and sensitive data from evolving threats.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://www.cisa.gov/news-events/alerts/2025/03/11/cisa-adds-six-known-exploited-vulnerabilities-catalog

TATA COMMUNICATIONS

New Elysium ransomware variant emerges, linked to the Ghost Cring family

Cybersecurity researchers have uncovered a new ransomware variant, dubbed Elysium, belonging to the notorious Ghost Cring family. This sophisticated malware targets both individuals and organisations, encrypting critical files and demanding ransom payments for decryption. Elysium employs advanced evasion techniques, making detection and mitigation challenging for traditional security tools. The ransomware spreads through phishing campaigns, malicious attachments, and exploit kits, often exploiting unpatched vulnerabilities in software. Once inside a system, it disables security features and exfiltrates sensitive data before encrypting files, adding pressure on victims to pay the ransom.

Analysis highlights the growing complexity of ransomware threats and underscores the importance of proactive defences, including regular software updates, employee training, and robust backup strategies. Organisations are urged to enhance their cybersecurity posture to combat evolving threats like Elysium and prevent potentially devastating financial and operational impacts.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://www.netskope.com/blog/analyzing-elysium-a-variant-of-the-ghost-cring-ransomware-family

TATA COMMUNICATIONS

FBI, CISA, and MS-ISAC issue joint warning on surge in Medusa ransomware attacks

The Federal Bureau of Investigation (FBI), CISA, and Multi-State Information Sharing and Analysis Center (MS-ISAC) have issued a joint advisory warning organisations about a sharp rise in Medusa ransomware attacks. This aggressive malware targets businesses globally, encrypting critical data and demanding hefty ransom payments, often in the millions. Medusa operators employ double extortion tactics, threatening to leak stolen data if ransoms are not paid. The ransomware primarily infiltrates systems through phishing emails, exploited vulnerabilities, and compromised remote desktop protocols (RDP). High-risk sectors include healthcare, education, and critical infrastructure.

Authorities urge organisations to implement robust cybersecurity measures, such as multi-factor authentication, regular software updates, and employee training. Immediate reporting of incidents is also emphasised to mitigate damage and disrupt attacker operations. The advisory highlights the escalating ransomware threat and the need for collective vigilance to safeguard sensitive data and infrastructure.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://securityonline.info/fbi-cisa-and-ms-isac-warn-organizations-about-medusa-ransomware-attacks/

TATA COMMUNICATIONS

P*zdec ransomware threatens data security, requires immediate action

A new ransomware strain, P*zdec, has emerged as a significant threat to individuals and organisations, encrypting files and demanding ransom payments for decryption. This malicious software infiltrates systems through phishing emails, malicious attachments, and exploit kits, often targeting outdated software vulnerabilities. Once inside, it locks critical data and displays a ransom note, pressuring victims to pay in cryptocurrency. Cybersecurity experts strongly advise against paying the ransom, as it does not guarantee file recovery and may encourage further attacks. Instead, they recommend preventive measures such as regular data backups, robust antivirus software, and employee training to recognise phishing attempts. For those already affected, removal tools and guides are available to eliminate the ransomware and restore systems.

The rise of P*zdec ransomware underscores the importance of proactive cybersecurity practices. Authorities urge users to update software, avoid suspicious links, and implement strong security protocols to protect against evolving digital threats.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://www.cyclonis.com/remove-pzdec-ransomware/

TATA COMMUNICATIONS

GitLab issues urgent patches for critical authentication bypass vulnerabilities

GitLab has released urgent security updates to address two critical authentication bypass vulnerabilities, identified as CVE-2025-25291 and CVE-2025-25292. These flaws, affecting both GitLab Community Edition (CE) and Enterprise Edition (EE), could allow attackers to bypass authentication mechanisms and gain unauthorised access to sensitive repositories, pipelines, and user data. The vulnerabilities, rated with CVSS scores of 9.9, pose a significant risk to organisations relying on GitLab for version control and DevOps operations. Exploitation could lead to data breaches, code theft, or malicious code injection, potentially disrupting critical workflows.

GitLab has strongly urged all users to immediately update to the latest versions – 16.7.8, 16.6.7, and 16.5.9 – to mitigate these risks. The company also recommended reviewing access logs for suspicious activity and enforcing multi-factor authentication as additional safeguards. This incident highlights the importance of timely software updates and robust security practices to protect against evolving cyber threats.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	GitLab Community Edition (CE), GitLab Enterprise Edition (EE)

Source - https://securityonline.info/gitlab-urgently-patches-critical-authentication-bypass-flaws-cve-2025-25291-cve-2025-25292/

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today's cyber threat landscape.

Book your visit