Promoting a Secure and Resilient Internet: Abuse Elevation Control Mechanism

Fabrice TEUGUIA

***Abstract:** The Abuse Elevation Control Mechanism (AECM) is a critical cybersecurity concern, as it allows attackers to bypass security controls and gain unauthorized elevated privileges. This research explores attackers' primary methods to exploit compromised credentials, including account takeover, credential stuffing, and malware installation. It also highlights key techniques such as bypassing User Account Control (UAC) and exploiting setuid/setgid on Unix-like systems. The article discusses mitigation strategies, including audit and monitoring, privileged account management, and execution prevention. Finally, it provides insights into the future of AECM, emphasizing the increasing sophistication of attacks, emerging attack vectors, and stronger defensive mechanisms. This work aims to inform cybersecurity professionals about the risks of AECM and provide actionable strategies to mitigate these threats.*

***Keywords:** Cyberattacks, Privilege Escalation, Security Standards, Ethical Hacking, Data Protection*

Abbreviations:
AECM: Abuse Elevation Control Mechanism
UAC: User Account Control
TCC: Transparency, Consent, and Control
GDPR: General Data Protection Regulation
CCPA: California Consumer Privacy Act
AI: Artificial Intelligence
DDoS: Distributed Denial of Service
ATTACK: Adversarial Tactics, Techniques, and Common Knowledge
CEO: Chief Executive Officer
DLL: Dynamic Link Library

I. INTRODUCTION

In today's interconnected digital landscape, ensuring the security and resilience of systems against cyber threats is paramount. Among these threats, the Abuse Elevation Control Mechanism (AECM) stands out as a significant risk. AECM involves exploiting features within operating systems or applications to enable users to elevate their privileges or gain higher levels of control, such as administrative rights. This circumvents security controls and grants unauthorized access to sensitive system functions, files, or data. Understanding the intricacies of AECM, including its exploitation methods and mitigation strategies, is crucial for cybersecurity professionals and organizations aiming to protect their assets.

II. OVERVIEW AND METHODOLOGY

This article synthesizes existing knowledge and reports from reputable cybersecurity frameworks like the MITRE ATTACK framework, alongside real-world examples and industry insights. The methodology involves a comprehensive review of documented attack techniques, analysis of security vulnerabilities, and examination of mitigation strategies proposed by cybersecurity experts. This approach aims to provide a holistic understanding of the AECM landscape.

The overview includes:

- Explanation of the core concept of AECM and its significance in the context of cyberattacks.
- Examination of how compromised credentials serve as a primary attack vector for AECM.
- Identification of key techniques employed by attackers to abuse elevation control mechanisms.
- Discussion of strategies for organizations to reduce the risks associated with AECM.

III. RESULTS AND DISCUSSION

A. Exploiting Compromised Credentials

Compromised credentials are a significant entry point for attackers seeking to abuse elevation control mechanisms. According to MITRE ATTACK FRAMEWORK [1], this technique allows adversaries to bypass mechanisms that control the elevation of privileges, enabling them to gain higher-level permissions on a system. Compromised credentials can be used for a variety of malicious purposes, affecting personal security, organizational integrity, and overall trust in digital systems. Some of the primary ways in which compromised credentials may be exploited are:

i. *Account Takeover:* Attackers can use stolen credentials to gain unauthorized access to user accounts, allowing them to impersonate legitimate users. They often result from a customer or employee unintentionally sharing sensitive information, which makes it available to bad actors.

ii. *Credential Stuffing Attacks:* Cybercriminals often use lists of compromised credentials obtained from previous data breaches to attempt to log into multiple accounts across different platforms. This technique exploits the tendency of users to reuse passwords, making it easier for attackers to gain access to various services [2].

iii. *Access to Sensitive Data:* Once attackers gain access to an account, they can steal sensitive information such as personal identification details, financial data, and proprietary business information.

Manuscript received on 22 January 2025 | First Revised Manuscript received on 21 February 2025 | Second Revised Manuscript received on 16 March 2025 | Manuscript Accepted on 15 April 2025 | Manuscript published on 30 April 2025.

*Correspondence Author(s)
Fabrice TEUGUIA*, Cabinet Riding-Up, Programme PCP-ACEFA, Cameroun. Email ID: fteuguia@gmail.com, fteuguia@pcpacefa.org, ORCID ID: 0009-0003-1530-6758

iv. *Installation of Malware:* Attackers may use compromised accounts to install malware on the victim's devices, which can further compromise the security of the individual or organization and lead to data breaches. SILVERFORT reports that, in 2018, Nintendo's intendo Network suffered a breach that compromised over 300,000 accounts. Login credentials were stolen and used to make fraudulent purchases [3].

v. *Facilitating Phishing Attacks:* Compromised credentials, can be used to launch phishing campaigns from legitimate accounts [4], tricking other users into providing their sensitive information or credentials (CEO Fraud, general and spear Phishing) [5].

vi. *Manipulating Trust:* By using compromised accounts, attackers can manipulate trust relationships, leading to further breaches within an organization or among individuals who believe they are communicating with a legitimate user [2].

vii. *Internal Network Access:* In organizational contexts, compromised credentials can allow attackers to move laterally within a network, accessing multiple systems and data repositories, which can lead to widespread damage and data loss [6]. On the website of Cloudflare [2] we can read that KILLNET, a pro-Russian hacktivist group [7], commits acts of cyber warfare via botnet-powered DDoS attacks [8].

B. Key Techniques Used by Attackers

Adversaries employ various methods to abuse elevation controls. Some of the key techniques they are using are:

i. *Bypass User Account Control (UAC):* Attackers can exploit weaknesses in UAC to execute commands with elevated privileges without user consent. This may involve using legitimate applications or scripts that do not trigger UAC prompts.

ii. *Setuid and Setgid Exploits:* On Unix-like systems, files with the setuid or setgid bits set can allow users to execute them with the permissions of the file owner or group. Attackers may create or manipulate such files to gain elevated access.

iii. *Sudo and Sudo Caching:* Exploiting misconfigurations in the sudoers file can allow attackers to execute commands as a superuser without proper authentication. This includes leveraging cached credentials to bypass password prompts.

iv. *Temporary Elevated Cloud Access:* In cloud environments, adversaries may exploit temporary access tokens or permissions to gain elevated privileges, allowing them to perform unauthorized actions within cloud services.

v. *TCC Manipulation on Mac OS:* Attackers can manipulate the Transparency, Consent, and Control (TCC) database to grant their applications elevated permissions without user prompts. This can involve using system applications to execute malicious payloads or modifying the TCC database directly.

C. Mitigation Strategies

Organizations can implement several strategies to mitigate risks associated with AECM:

i. *Audit and Monitoring:* Regularly check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate - Monitor executed commands and arguments that may circumvent mechanisms designed to control elevated privileges and gain higher-level permissions - On Linux systems, use auditd to alert when a user's actual ID and effective ID are different, which can indicate abuse of setuid or setgid bits [1].

ii. *Restrict Files and Directory Permissions:* Minimize the number of programs with setuid or setgid bits set across the system to reduce potential damage if an application is compromised - Ensure the sudoers file is strictly edited such that passwords are always required and users cannot spawn risky processes as higher-privileged users [1].

iii. *Execution Prevention:* Configure system settings to prevent applications from running that haven't been downloaded from legitimate repositories, which may help mitigate some abuse issues - Do not allow unsigned applications to be run, which may also mitigate some risk [1].

iv. *Privileged Account Management:* Remove users from the local administrator group on systems. Requiring a password ensures adversaries must know the password to run anything in the sudoers file - Set the sudo timestamp timeout to 0 to require the user to input their password every time sudo is executed [1].

v. *User Account Control (UAC):* Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities with techniques such as DLL Search Order Hijacking [1].

IV. DISCUSSION AND FUTURE TRENDS

The future of the "Abuse Elevation Control Mechanism" technique will likely see a cat-and-mouse game between attackers and defenders, with each side constantly evolving. While attackers will find new ways to exploit these mechanisms, defenders will continue to strengthen their systems, guided by technological advances, regulation, and collaboration. The ongoing battle will shape the cybersecurity landscape, influencing how systems are designed, managed, and secured. Regarding that, some key considerations are:

A. Increased Sophistication of Attacks

i. *Advanced Automation:* Tools like Meterpreter, Cobalt Strike, and Empire may continue to develop automated methods for privilege escalation, making it easier for attackers to exploit vulnerabilities in elevation controls.

ii. *AI-Driven Attacks:* The use of artificial intelligence and machine learning by attackers could automate the identification of potential weaknesses in elevation control mechanisms, making attacks more targeted and efficient.

iii. *Exploitation of New Vulnerabilities:* As operating systems and applications evolve, new vulnerabilities may emerge that can be exploited to bypass existing elevation controls, necessitating continuous monitoring and adaptation of security measures.

iv. *The Vulgarization of Attack Techniques in Social Networks:* This trend has been facilitated by the increasing accessibility of information and tools that make it easier for malicious actors to launch attacks. The availability of online tutorials and forums has made it easier for individuals with limited or advanced technical skills to learn and execute these attack techniques.

B. Emergence of New Attack Vectors

i. *Cloud Environments:* With the growth of cloud computing, attackers may focus on exploiting privilege escalation in cloud environments, where access controls are often complex and can be misconfigured

ii. *Containerization and Microservices:* As organizations adopt containerization and microservices, attackers may find new ways to abuse elevation control mechanisms within these environments, potentially escaping containers or escalating privileges across distributed systems.

iii. *Machine Learning:* Integrating machine learning into security systems may enhance the ability to detect and respond to privilege escalation attempts in real-time.

C. Stronger Defensive Mechanisms

i. *Enhanced User Account Control (UAC) and Sudo Implementations:* Future iterations of UAC in Windows and `sudo` in Unix-like systems might include more granular controls, better auditing, and increased resistance to known bypass techniques.

ii. *Zero Trust Security Models:* Adopting zero trust architectures will emphasize the importance of continuous verification, making it harder for attackers to abuse elevation controls even if they initially gain access to a system.

iii. *Application Vetting:* Organizations may adopt more rigorous application vetting processes to ensure that applications do not unnecessarily request elevated permissions, reducing the attack surface.

D. Regulatory and Compliance Pressures

i. *Stricter Compliance Requirements:* Regulatory frameworks like GDPR, CCPA, and others might impose stricter requirements on organizations to prevent and mitigate the risks of privilege escalation, leading to more robust security practices.

ii. *Increased Accountability:* As governments and industries push for stronger cybersecurity measures, organizations might be held more accountable for failing to protect against such abuses, leading to the implementation of more stringent security controls.

E. Growing Awareness and Education

i. *Security Training:* There will be a continued emphasis on educating developers and system administrators about the risks associated with elevation control mechanisms, leading to better design and configuration of systems.

ii. *Improved Detection Tools:* Security tools will continue to advance, offering better detection of abuse attempts through behavioral analysis and anomaly detection, reducing the window of opportunity for attackers.

iii. *Behavioral Monitoring:* Increased focus on monitoring for anomalous behavior that may indicate attempts to abuse elevation controls, such as unusual command executions or process creations.

F. Legal and Ethical Considerations

i. *Ethical Hacking and Bug Bounty Programs:* The growth of ethical hacking initiatives and bug bounty programs will encourage the discovery and disclosure of potential elevation control abuses, leading to quicker fixes and more secure systems.

ii. *Legal Consequences:* As laws around cybersecurity tighten, the legal ramifications for abusing elevation control mechanisms might become more severe, acting as a deterrent for attackers.

iii. *Threat Intelligence Sharing:* Increased collaboration between organizations, governments, and security researchers will lead to more timely and effective sharing of threat intelligence related to abuse techniques.

V. CONCLUSION

The Abuse Elevation Control Mechanism (AECM) represents a significant cybersecurity threat, enabling attackers to bypass security controls and gain unauthorized access to sensitive systems and data. This article has explored the primary methods of exploiting compromised credentials, key techniques for abusing elevation controls, and strategies to mitigate these risks. The future of AECM will likely involve a continuous evolution of attack techniques and defensive measures, driven by technological advancements, regulatory pressures, and increased awareness.

Organizations must adopt proactive strategies, such as audit and monitoring, privileged account management, and zero trust architectures, to protect against AECM. By staying informed about emerging threats and implementing robust security practices, organizations can reduce the risks associated with AECM and enhance their overall cybersecurity posture.

DECLARATION STATEMENT

I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed solely.

REFERENCES

1. T. M. Corporation, «Abuse Elevation Control Mechanism,» 01 2020. [En ligne]. Available: https://attack.mitre.org/techniques/T1548/. [Accès le 08 2024]
2. D. B. S. Z. Michael Tremante, «The state of application security in 2023,» 03 2023. [En ligne]. Available:

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

https://blog.cloudflare.com/application-security-2023/. [Accès le 08 2024]

3. «What is Compromised Credential?,» [En ligne]. Available: https://www.silverfort.com/glossary/compromised-credential/. [Accès le 08 2024]
4. C. Crane, «Compromised Credentials: 7 Ways to Fight Credential Attacks,» 07 2023. [En ligne]. Available: https://www.thesslstore.com/blog/compromised-credentials-ways-to-fight-credential-attacks/. [Accès le 08 2024]
5. Kalra, Y., Upadhyay, S., & Patheja, Dr. P. S. (2020). Advancements in Cyber Attacks and Security. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 4, pp. 1520–1528). DOI: https://doi.org/10.35940/ijitee.d1678.029420
6. M, D. D., S, B. K., & Lal, D. (2020). Major Hurdles of Cyber Security in 21st Century. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 3, pp. 1470–1476). DOI: https://doi.org/10.35940/ijeat.c5135.029320
7. Lakshmi, N. N., P. Karthik, Sai, P. S., & Vishal, A. S. (2024). Implementation of DOS Attack Using NS2. In International Journal of Emerging Science and Engineering (Vol. 12, Issue 6, pp. 1–4). DOI: https://doi.org/10.35940/ijese.f9859.12060524
8. Sasikumar, H. (2021). DDoS Attack Detection and Classification using Machine Learning Models with Real Time Dataset Created. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 9, Issue 5, pp. 145–153). DOI: https://doi.org/10.35940/ijrte.e5217.019521

AUTHOR'S PROFILE

Fabrice TEUGUIA is an expert in Foresight and IT Project Management. He has been involved in many monitoring and evaluation projects, information system charters and policies, and IT Projects. Now he is engaged in the association of future science and IT science. Fabrice TEUGUIA has a visionary goal, to drive innovation in standards and policies over the next decade.

Some of my works:

« Initiation à l'Informatique et Internet » par les éditions universitaires européennes (2018). ISBN : 978-613-8-42544-1

« La virtualisation, le télétravail, les managers » Décembre 2020 par Amazon ISBN-13 : 979-8587680418

« Les traces numériques dans 10 ans » par les éditions universitaires européennes (2021). ISBN : 978-620-2-26874-5

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/ or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.