# Critical vulnerability identified in Lightning AI Studio raises security concerns



In a notable development in the realm of artificial intelligence, researchers from Noma Security have identified a high-severity Remote Code Execution (RCE) vulnerability within Lightning AI Studio, a popular platform used for AI development. The vulnerability, which has garnered a CVSS score of 9.4, poses substantial risks to users, enabling attackers to execute arbitrary commands with root privileges. This, in turn, raises concerns around potential data exfiltration and system compromise.

The critical vulnerability was associated with a concealed URL parameter named "command" embedded in the terminal functionality of Lightning AI Studio. Although this parameter was hidden from users, malicious actors could exploit it by crafting a Base64-encoded payload. By appending this payload to user-specific URLs, attackers were able to execute harmful commands due to the platform's lack of input sanitization. For example, through this exploit, an attacker could issue a command to recursively delete files or access sensitive AWS metadata, such as access tokens, redirecting that data to a remote server.

The exploit required publicly available information, including usernames and studio paths, which could be extracted from Lightning AI's shared studio templates. As a result, victims could be targeted by means of malicious links, distributed through emails or public forums, which would trigger the exploit upon a user's click.

Lightning AI Studio, operating as a cloud-based platform for AI development, supports a variety of workflows, including training and deployment. Its popularity among enterprises and developers is attributed to features such as a Visual Studio Code-like interface and persistent environments. However, the vulnerability discovered within its handling of user-controllable inputs, specifically hidden URL parameters, has brought into question the platform's overall security.

The URL schema for Lightning AI Studio includes variables such as PROFILE\_USERNAME and STUDIO\_PATH, which are used to uniquely identify user studios. Attackers managed to exploit these variables, creating malicious URLs that could redirect authenticated users to terminals equipped with detrimental commands.

The ramifications of this exploit were significant. Attackers had the potential to execute arbitrary commands, exfiltrate sensitive data, and compromise filesystems, including the deletion or alteration of key system files, thereby disrupting operational integrity. Given that Lightning AI Studio is integral to enterprise-grade AI workflows, the exploitation risk extended to sensitive AI models and data pipelines across environments shared by multiple users.

Following a responsible disclosure on October 14, 2024, Noma Security worked closely with Lightning AI to resolve the vulnerability, leading to the rollout of a fix by October 25, 2024. Key insights gleaned from this incident underscore the necessity for rigorous input validation, adherence to the principle of least privilege, and a prohibition against the execution of user-controlled inputs to avoid command injection vulnerabilities.

This incident serves as a significant reminder of the importance of embedding robust security measures into the AI development lifecycle. As innovation within the industry accelerates, the resilience of platforms like Lightning AI is crucial. Noma Security's role in pinpointing and addressing such vulnerabilities illustrates their commitment to safeguarding the AI ecosystem from emerging threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://noma.security/noma-research-discovers-rce-vulnerability-in-ai-development-platform-lightning-ai/> - This URL supports the claim about Noma Security discovering a Remote Code Execution (RCE) vulnerability in Lightning AI Studio, which allowed attackers to execute arbitrary commands with root privileges.
* <https://gbhackers.com/hackers-can-exploit-ai-platform-to-achieve-root-access/> - This article corroborates the details of the RCE vulnerability, including its CVSS score of 9.4 and the exploitation method using a hidden 'command' URL parameter.
* <https://cyberscoop.com/lightningai-vulnerability-noma-cloud-phishing/> - This URL provides additional information on the vulnerability, including how it was patched and the potential for attackers to gain root access and control over user studios.
* <https://www.noahwire.com> - This is the source mentioned in the text, though it does not directly support specific claims about the vulnerability.
* <https://noma.security/noma-research-discovers-rce-vulnerability-in-ai-development-platform-lightning-ai/> - This URL further explains the attack flow and how attackers could exploit publicly accessible information to target victims.
* <https://gbhackers.com/hackers-can-exploit-ai-platform-to-achieve-root-access/> - This article details the potential consequences of the exploit, such as data exfiltration and system compromise.
* <https://cyberscoop.com/lightningai-vulnerability-noma-cloud-phishing/> - This URL discusses the collaboration between Noma Security and Lightning AI to resolve the vulnerability.
* <https://noma.security/noma-research-discovers-rce-vulnerability-in-ai-development-platform-lightning-ai/> - This article highlights the importance of robust security measures in AI development platforms like Lightning AI Studio.
* <https://gbhackers.com/hackers-can-exploit-ai-platform-to-achieve-root-access/> - This article emphasizes the risks associated with the lack of input sanitization and the exploitation of hidden URL parameters.