Elastic rejects claims of a zero-day RCE flaw in Defend EDR - Against Inva

Data: 2025-08-19 20:33:14

Autor: Inteligência Against Invaders

Enterprise search and security company Elastic is rejecting reports of a zero-day vulnerability

impacting its Defend endpoint detection and response (EDR) product.

The company's statement follows a blog post froma company called AshES Cybersecurityclaiming to have discovereda remote code execution (RCE) flaw in Elastic Defend that would allow an attacker to bypass EDR protections.

Elastic's Security Engineering team "conducted a thorough investigation" but could not find "evidence supporting the claims of a vulnerability that bypasses EDR monitoring and enables remote code execution."

Zero-day claims

According to AshES Cybersecurity's write-up from August 16,a NULL pointer dereference flaw in Elastic Defender's kernel driver, 'elastic-endpoint-driver.sys' could be weaponized to bypassEDR monitoring, enableremote code execution with reduced visibility, and establishpersistence on the system.

"For proof-of-concept demonstration, I used a custom driver to reliably trigger the flaw under controlled conditions," theAshES Cybersecurity researcher says.

To show the validity of the finding, the company published two videos, one showing Windows crashing because Elastic's driver failed, and another showing the alleged exploit starting calc.exe without Elastic's Defend EDR taking action.

"The Elastic driver 0-day is not just a stability bug. It enables a full attack chain that adversaries can exploit inside real environments," the researcher claims.

Elastic's rejection

After evaluatingAshES Cybersecurity's claims and reports, Elastic was not able to reproduce the vulnerability and its effects.

Furthermore, Elastic says that the multiple reports it received fromAshES Cybersecurity for the alleged zero-day bug "lacked evidence of reproducible exploits."

"Elastic Security Engineering and our bug bounty triage team completed a thorough analysis trying to reproduce these reports and were unable to do so. Researchers are required to share reproducible proof-of-concepts; however, they declined" – Elastic

AshES Cybersecurityconfirmed that they chose not to send the PoC to Elastic or the company’s affiliates.

Elastic says that the researcher did not share the full details for the vulnerability and instead decided to make their claims public instead of following the principles of coordinated disclosure.

Elastic reaffirmed that they take all security reports seriously and, starting 2017, paid more than $600,000 to researchers through the company’s bug bounty program.

[IMAGEM REMOVIDA]