Adobe Acrobat Vulnerabilities Allow Remote Code Execution

Security researchers from Cisco Talos have discovered multiple vulnerabilities in Adobe Acrobat, potentially allowing attackers to execute arbitrary code or access sensitive information. These flaws primarily stem from issues in the software’s font handling functionality.

The identified vulnerabilities include out-of-bounds read flaws and a memory corruption issue, which could be exploited through maliciously crafted PDF files.

CVE-2025-27163 & CVE-2025-27164 may lead to sensitive information disclosure. Attackers could leverage these weaknesses to gain unauthorized access to system data.
CVE-2025-27158 is a memory corruption vulnerability caused by an uninitialized pointer in Adobe Acrobat’s font processing. If exploited, this flaw could allow an attacker to execute arbitrary code.

The susceptibilities affect various versions of Adobe Acrobat, though specific impacted versions have not yet been disclosed in detail. If successfully exploited, these exposure could allow attackers to steal sensitive data from affected systems. It can remotely execute malicious code and gain unauthorized system access.

Given the widespread use of Adobe Acrobat for PDF management, these security issues pose a significant risk to individual users and businesses alike.

To protect against potential exploits, users and organizations should take immediate action. Adobe has released patches addressing these harms. Users are urged to apply the latest security updates promptly. Avoid opening PDF documents from untrusted or unknown sources. Implement endpoint security solutions and intrusion detection systems to mitigate exploitation risks.