IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, March 2025
Impact Factor: 7.67

Unraveling the 2024 CrowdStrike Incident: How a Security Patch Led to Global System Failure and Blue Screen of Death

Venkata Baladari
Sr. Software Developer, Newark, Delaware
vrssp.baladari@gmail.com

Abstract: *The 2024 CrowdStrike Cybersecurity incident resulted in a worldwide IT disruption impacting millions of Microsoft Windows systems. In July 2024, a faulty update of CrowdStrike's Falcon Endpoint Detection and Response (EDR) software caused widespread system crashes known as the "Blue Screen of Death" (BSOD). The event caused severe disruptions to major industries such as aviation, financial services, healthcare and emergency response systems resulting in operational shutdown, financial setbacks and global safety concerns.*

This study presents a detailed examination of the CrowdStrike incident, focusing on the technical issues, global effects and legal consequences. The research delves into the weakness of centralized cybersecurity systems, emphasizing the dangers of putting too much trust in single-point security services. The research highlights the significance of strict testing protocols, comprehensive cybersecurity frameworks, and risk assessment strategies enhancing future cybersecurity preparedness. The CrowdStrike incident presents a compelling case study in global cybersecurity risk management, prompting organizations to reassess redundancy measures, failover mechanisms, and more decentralized security architectures in order to protect critical IT systems..

Keywords: CrowdStrike, Cybersecurity, Cyber Risk Management, Incident Response, Regulatory Compliance, Blue Screen of Death (BSOD)

Copyright to IJARSCT
www.ijarsct.co.in

ISSN 2581-9429 IJARSCT
DOI: 10.48175/IJARSCT-24524