INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC

DOI No. 10.5281/zenodo.16794479

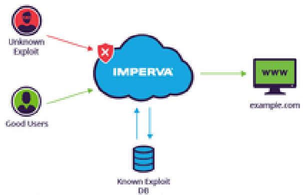
JULY 2025

CYBER BULLETIN

The Cyber Fortress

FortiWeb Exploited 1.

ZERO-DAY RCE EXPLOIT



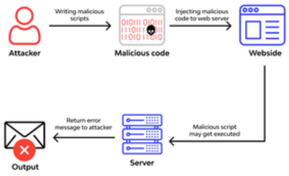
TARGET: Organizations using Fortinet FortiWeb WAF, Web portals/APIs with sensitive financial or customer data.

IMPACT: Full system takeover & data theft. Malware deployment including ransomware and cryptominers.

MITIGATION: Update to patched firmware immediately. Restrict admin interface and enable strict WAF rules.

Microsoft SharePoint RCE 2.

UNAUTHENTICATED RCE


Attacker
Writing malicious scripts
Malicious code
Injecting malicious code to web server
Webside
Malicious script may get executed
Server
Return error message to attacker
Output

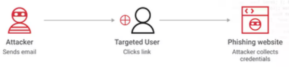
TARGET: Internet-exposed collaboration portals without patches. On-premises SharePoint servers in enterprises.

IMPACT: Remote command execution without credentials. Lateral network movement and sensitive data theft.

MITIGATION: Apply Microsoft's July 2025 patch. Restrict SharePoint access to internal/VPN networks.

Nation-State Cyber Threats 3.

SPEAR-PHISHING



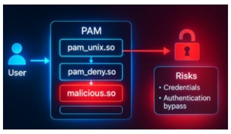
TARGET: Energy, water, and transportation sectors and ICS/OT devices and associated enterprise IT systems.

IMPACT: Theft of operational blueprints and sensitive designs and potential sabotage and service shutdowns.

MITIGATION: Patch ICS/OT systems and enforce Zero Trust and enable MFA and deploy IDS/IPS monitoring.

PAM Backdoor Threat 4.

PAM IMPLANTATION



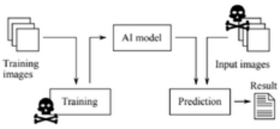
TARGET: Linux/UNIX systems using PAM authentication and critical infrastructure with PAM-based access control.

IMPACT: Stealthy long-term compromise. Espionage and lateral movement into core systems.

MITIGATION: Enable file integrity monitoring. Audit logs and restrict module installation to trusted sources.

AI Endpoint Threats 5.

AI MODEL EXPLOITATION



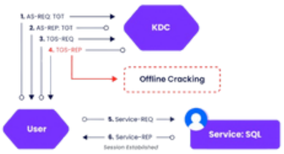
TARGET: Cloud/SaaS services with security gaps. Endpoints targeted via phishing or AI model attacks.

IMPACT: Large-scale breaches and operational downtime. AI-driven exploitation of business systems.

MITIGATION: Use AI-powered EDR/XDR tools to quickly spot and stop threats. Set up continuous monitoring for both cloud and endpoint systems.

Kerberoasting Detections 6.

KERBEROS CRACKING



TARGET: Active Directory environments with service accounts that have SPNs. Privileged accounts vulnerable to offline password cracking.

IMPACT: Attackers gain privileges by cracking service account passwords. Credential theft leading to sensitive data exposure.

MITIGATION: Monitor Kerberos traffic with behavior analytics to detect anomalies. Use least privilege, audit SPNs, and enable AES encryption with automated password rotation.

INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC

DOI No. 10.5281/zenodo.16794479

JULY 2025

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

CYBER SECURITY
POSTER OF THE DAY

Enable Multi-Factor Authentication (MFA) on all important accounts

AI-powered phishing attacks are increasingly sophisticated and can bypass weak passwords

#MFA
#AccountSecurity
#AIFraud

Supported by

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
Digital India
myGov मेरी सरकार
Indian Cyber Crime Coordination Centre
सी डैक CDAC

CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS
MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TALHA
STUDENTS COORDINATORS
ANAMTA ANSARI | AREEBA KHAN

Prof.(Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application