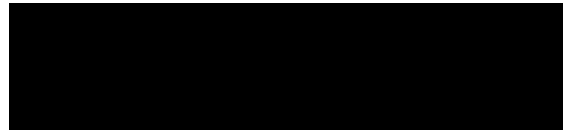

Cyber Bulletin, January 2026 Edition by Cyber Awareness Club, Department of Computer Application

Communication Cell IUL <communications@iul.ac.in>

Thu, Feb 26, 2026 at 2:09 PM

Bcc: faculty@iul.ac.in



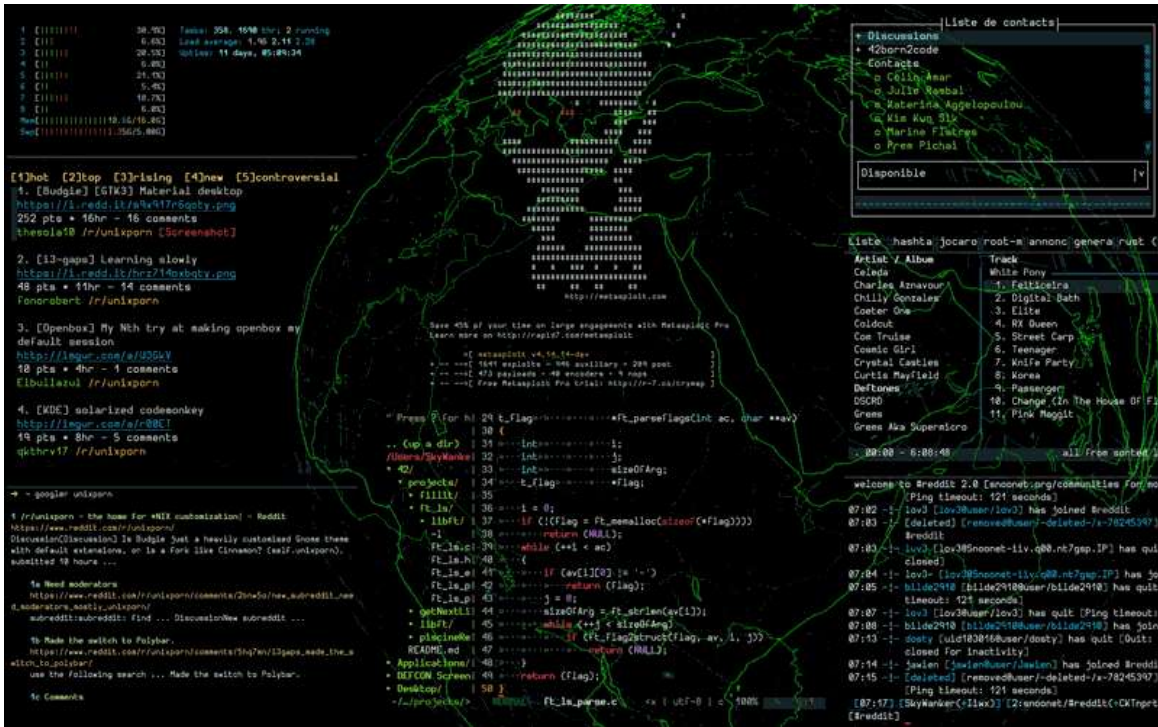
Dear All,

Welcome to the **Cyber Bulletin – January 2026**. This edition highlights the growing threat of **zero-day vulnerabilities** that are actively being exploited across major technologies at the start of the year. Cyber attackers targeted widely used platforms including **Microsoft Office, Windows systems, Cisco communication tools, Ivanti Endpoint Manager Mobile, and VMware ESXi environments**, demonstrating how critical digital infrastructure remains at risk. These attacks enabled remote code execution, privilege escalation, memory data leakage, and system compromise through malicious documents, phishing emails, and network-based exploits.

The bulletin emphasizes that modern cyber threats are becoming more advanced, with **state-linked groups** and **ransomware operators** leveraging undisclosed flaws before organizations can fully defend themselves. Such incidents underline the importance of **timely patching, system hardening, user awareness against phishing, and continuous monitoring** to prevent large-scale damage. Cybersecurity is not just a technical need but a **shared responsibility** for maintaining digital trust and resilience.

 **Stay Alert • Stay Safe • Report Cybercrime – @1930**

Stay informed • Stay secure • Stay cyber-safe



👥 Cyber Awareness Club

Mentor

Prof. (Dr.) Mohammad Faisal
Head, Department of Computer Application

Faculty Coordinators

Mr. Shubham Kumar
Assistant Professor

Mr. Faizan Mahmood
Assistant Professor

Mr. Mohd Talha
Teaching Support Staff

Student Coordinators

Anamta Ansari
BCA Second Year

Areeba Khan
BCA Second Year

Anwar Ahmad
BCA Second Year

Hashmat Zahra
BCA Second Year

Hera Fatima
BCA Second Year



CYBER BULLETIN



CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION
INTEGRAL UNIVERSITY, LUCKNOW

JANUARY 2026

DOI No. 10.5281/zenodo.1861851

ZERO-DAY NEWS



Ivanti EPMM RCE Zero-Day

Attackers are actively exploiting critical zero-day vulnerabilities in Ivanti Endpoint Manager Mobile to gain unauthenticated remote code execution, resulting in full server compromise, exposure of sensitive enterprise & device data across internal corporate networks.

Cause: Actively exploited zero-day vulnerabilities

[readme](#)



VMware ESXi Sandbox

Ransomware gangs are actively exploiting a high-severity VMware ESXi sandbox escape zero-day (CVE-2025-22225), patched in March 2025, allowing attackers with VM privileges to execute kernel-level attacks and escape VMs, affecting widely deployed VMware enterprise products.

Cause: Exploited VMware ESXi zero-day

[readme](#)



MS Office OLE Zero-Day Exploit

Attackers are exploiting a critical Microsoft Office zero-day (CVE-2026-21509) that allows specially crafted documents to run malicious code when opened without warnings or macros. The flaw bypasses security protections enables remote connections via Shell.Explorer.1 & allows system compromise.

Cause: OLE/COM Object Exploit

[readme](#)



APT28 Targets Office Vulnerability

Russian-linked APT28 is actively exploiting Microsoft Office zero-day CVE-2026-21509 via phishing emails with malicious RTF files, bypassing OLE protections to deploy MiniDoor malware. Attacks target Eastern European governments despite emergency patches

Cause: Phishing emails with malicious RTF files.

[readme](#)



Cisco Unified RCE Zero-Day

The attack targets a critical Cisco zero-day like Unified CM, IM&P, Unity Connection and Webex calling. Hackers exploit improper input validation in the web management interface sending specially crafted HTTP requests to gain user-level access and escalate to root privileges allowing full control of the device.

Cause: Improper HTTP input validation.

[readme](#)



Windows DWM Zero-Day Attack

Attackers exploited a flaw in Windows Desktop Window Manager to leak sensitive system memory from compromised machines. While not allowing direct remote takeover the exposed information helped attackers bypass security protections enabling privilege escalation.

Cause: Memory disclosure via DWM buffer mishandling

[readme](#)

BEST PRACTICE

- Apply all vendor patches and updates immediately to fix known vulnerabilities and reduce zero-day exposure.
- Restrict admin and VM privileges with multi-factor authentication to prevent unauthorized access and privilege escalation.
- Segment critical networks and isolate sensitive systems to limit breach impact and lateral movement.
- Educate users on phishing and malicious documents to prevent social engineering and document-based exploits.
- Harden configurations, registry and applications to block common attack vectors like COM, HTTP and memory flaws.
- Continuously monitor logs endpoints and system activity to detect unusual behavior and respond promptly.



INTEGRAL UNIVERSITY
LUCKNOW - INDIA

A+ ACCREDITED BY NAAC

NABH ACCREDITED FOR MEDICAL SERVICES

NABL ACCREDITED FOR LABS

NBA & ICAR ACCREDITED FOR FOOD SAFETY

CG-PAVE ACCREDITED

28

CYBER BULLETIN



CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION
INTEGRAL UNIVERSITY, LUCKNOW

JANUARY 2026

DOI No. 18-5281/zenodo.18618563



Ministry of Electronics and INFORMATION TECHNOLOGY



Digital India
Power To Empower



www.isea.gov.in



STAY SAFE ONLINE
www.staysafeonline.in



SaferInternetday2026

Educate children about AI-generated online personas that may be deceptive

#ChildSafety
#OnlinePredators

Supported by



Stay Alert, Stay Safe, Report Cybercrime @1930

CYBER SAKCHHARTA ABHIYAN UNDER THE AEGIS OF CYBER AWARENESS CLUB

FACULTY COORDINATORS

MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TAL HA

STUDENTS COORDINATORS

ANAMTA ANSARI | ARBEBA KHAN | ANWAR AHMAD
HASHMAT ZAHRA | HERA FATIMA

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



This initiative contributes to the UN Sustainable Development Goals by promoting cybersecurity awareness, digital safety, and resilient technological infrastructure.

--

Dr. Mohammad Faisal
Professor & Head
Department of Computer Application
Integral University
Kursi Road, Lucknow 226026
Email: headca@iul.ac.in
Mobile No: 9984171083



INTEGRAL UNIVERSITY
LUCKNOW - INDIA
ACCREDITED BY NAAC

