

DX CYBER -BULLETIN-

2nd edition | August, 2022



GOVERNMENT OF INDIA INITIATIVE ON CYBER CRIME REPORTING

The **National Cyber Crime Reporting Portal** is an initiative of Government of India to facilitate victims/complainants to report cyber-crime complaints online. **If you are a victim of Cyber Crime:**

Helpline Number: **1930** | Register your complaint at <https://cybercrime.gov.in/>



CYBER SECURITY NEWS

How leaking of employee's passwords led to hacking of 140,000 credit card payment terminals

The Times of India | 2 August 2022

Hackers have reportedly stolen thousands of passwords to gain access to dashboards used to remotely manage and control thousands of credit card payment terminals manufactured by digital payments major Wiseasy. The report in TechCrunch

[Read more...](#)

Largest DDoS Attack Ever – 659.6 Million Packets Per Second

GBHackers on Security | 2 August 2022

In the past few weeks, an organization in Eastern Europe has been the victim of the biggest DDoS attack that the continent has ever experienced. During the past month, several DDoS attacks have been launched against the target, a customer of

[Read more...](#)

Singapore takes formal step towards setting up cyber defence unit

ZDNet | 2 August 2022

Singapore has passed amendments to two Bills that will clear the way for a new digital intelligence unit to be established as part of the country's armed forces. The government has described the move as necessary amidst intensifying "cyber

[Read more...](#)

77% of organizations expect to increase cybersecurity budget as attacks rise: Verizon Business study

The Economic Times | 3 August 2022

Over three-quarters (77%) of organizations expect to increase their cybersecurity budget again in the next 12 months on the back of rising cyberattacks which have resulted in data loss and downtime, according to the findings of a survey by Verizon

[Read more...](#)

Government withdraws Personal Data Protection Bill 2019, to present new bill

Money Control | 3 August 2022

The Centre on August 3 withdrew the Personal Data Protection Bill, 2019, and will be introducing a new Bill. The reason for withdrawal given by the Ministry of Electronics and Information Technology Minister Ashwini Vaishnaw to the members of the

[Read more...](#)

German Chambers of Industry and Commerce hit by 'massive' cyberattack

Bleeping Computer | 4 August 2022

The Association of German Chambers of Industry and Commerce (DIHK) was forced to shut down all of its IT systems and switch off digital services, telephones, and email servers, in response to a cyberattack. DIHK is a coalition of 79 chambers

[Read more...](#)

UK NHS suffers outage after cyberattack on managed service provider

Bleeping Computer | 5 August 2022

United Kingdom's National Health Service (NHS) 111 emergency services are affected by a significant and ongoing outage triggered by a cyberattack that hit the systems of British managed service provider (MSP) Advanced. Advanced's Adastra

[Read more...](#)

Cisco Confirms It's Been Hacked by Yanluowang Ransomware Gang

The Hacker News | 12 August 2022

Networking equipment major Cisco on Wednesday confirmed it was the victim of a cyberattack on May 24, 2022, after the attackers got hold of an employee's personal Google account that contained passwords synced from their web browser. "Initial

[Read more...](#)

Xiaomi Phones with MediaTek Chips Found Vulnerable to Forged Payments

The Hacker News | 12 August 2022

Security flaws have been identified in Xiaomi Redmi Note 9T and Redmi Note 11 models, which could be exploited to disable the mobile payment mechanism and even forge transactions via a rogue Android app installed on the devices. Check Point said it

[Read more...](#)

Microsoft Employees Exposed Own Company's Internal Logins

Vice Media | 16 August 2022

Multiple people who appear to be employees of Microsoft have exposed sensitive login credentials to the company's own infrastructure on GitHub, potentially offering attackers a gateway into internal Microsoft systems, according to a

[Read more...](#)

BharatPay data breach: Personal data, transaction details of 37,000 users leaked online

The Economic Times | 17 August 2022

The compromised data includes user names, hashed passwords, mobile phone numbers, and UPI IDs. Official email IDs of Indian insurance and banking firm employees were also exposed. On August 13, CloudSEK's threat intelligence arm, XVigil,

[Read more...](#)

Google Play malware: If you've downloaded these malicious apps, delete them immediately

ZDNET | 18 August 2022

Cybersecurity researchers identify 35 apps, many downloaded over 100,000 times, that have been serving up malware to millions of Android users. Over two million Android users have downloaded a series of malicious apps that bypassed security

[Read more...](#)



CYBER SECURITY THREATS

VMware urges admins to patch critical auth bypass bug immediately

Bleeping Computer | 2 August 2022

VMware has warned admins today to patch a critical authentication bypass security flaw affecting local domain users in multiple products and enabling unauthenticated attackers to gain admin privileges. The flaw (CVE-2022-31656) was reported

[Read more...](#)

Google Patches Critical Android Bluetooth Flaw in August Security Bulletin

Infosecurity Magazine | 2 August 2022

Google published its monthly security bulletin for August on Monday, detailing the latest available patches for Android. A total of 37 vulnerabilities have been patched, including a critical security flaw in the System component that could lead to remote

[Read more...](#)

Cisco Business Routers Found Vulnerable to Critical Remote Hacking Flaws

The Hacker News | 3 August 2022

Cisco on Wednesday rolled out patches to address eight security vulnerabilities, three of which could be weaponized by an unauthenticated attacker to gain remote code execution (RCE) or cause a denial-of-service (DoS) condition on affected

[Read more...](#)

CISA Adds Zimbra Email Vulnerability to its Exploited Vulnerabilities Catalog

The Hacker News | 4 August 2022

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added a recently disclosed high-severity vulnerability in the Zimbra email suite to its Known Exploited Vulnerabilities Catalog, citing evidence of active exploitation.

[Read more...](#)

Microsoft Issues Patches for 121 Flaws, Including Zero-Day Under Active Attack

The Hacker News | 9 August 2022

As many as 121 new security flaws were patched by Microsoft as part of its Patch Tuesday updates for the month of August, which also includes a fix for a Support Diagnostic Tool vulnerability that the company said is being actively exploited in the

[Read more...](#)



CYBER EXPERT OPINIONS



Next-Generation Endpoint Protection: Due to Increase in work from home adoption and digital transformation strategy, it becomes uttermost important to equipped with necessary tool and technologies which will provide continuous visibility at a same time provide secure access to user in seamless manner.

End Point is a new parameter hence we must be implemented accordingly without complicating access or adding overhead to user. Hence, we must implement solution implemented from backend where we did not have much user engagement, this is applicable for endpoints, or server.

Next generation End Point protection solution which can protect endpoint from latest generation attack at same time equipped security team to perform detail analysis capabilities with relevant information and logs, it should be able to provide detail information about end point including application which are installed, running, or getting executed at OS or memory and more. Also, able to block at malicious activities and log at the same time. It should be able to integrate with other security solution and share relevant information.

Mr. Basil Dange

Chief Information Security Officer Risk Management, Aditya Birla Sun Life AMC Limited



Data Privacy perspective in India: As the technology grows, the vulnerabilities are accompanied with various risks in this Digital Age. The growing dependency on digital technologies is becoming a way of life, and at the same time, the collection of data using these technologies for surveillance operations has raised concerns. So, data privacy is the need of the hour which needs utmost priority to enable data protection to safeguard the environment.

Successful security transformation requires not only the right set of tools but the right expertise and guidance to drive the process for the best results!

Ms Kavitha Srinivasulu

Global Head - Cyber Risk & BFSI R&C, Tata Consultancy Services

Cyber Security Awareness: Password Security Tips

- Keep your password strong**
- Always change your password at regular intervals**
- Never share your password with anyone**
- Always log off your system**
- Never use the same password for each account**
- Protect yourself from shoulder surfing**



Cyber Raksha Kavach Dashboard

Total Registered	# of Sessions	# of Feedback
1,133	29	182
Content Satisfaction	Logistics Score	Faculty Score
4.52	4.22	4.58



Upcoming CII Cyber Security Training – Cyber Raksha Kavach

Time: 11 AM to 3 PM | Virtually on Microsoft Teams

2nd September 2022	6th September 2022	9th September 2022
Register now	Register now	Register now

For more information, contact

Mr. Mousam Khatri at mousam.khatri@cii.in
Mr. Ridham Tripathi at ridham.tripathi@cii.in

Follow us on

/Centre4DT
 /centre4dt/
 https://www.youtube.com/channel/UCwmUeXfSy0yzmMr_AAdcGnw

You are receiving this email because you signed up at www.ciidt.com

Our archives are at www.ciidt.com
Copyright © 2022 CII CDT, all rights reserved.
[Unsubscribe from this list](#)

Disclaimer: The views and opinions expressed in this newsletter are those of the speakers and do not necessarily reflect the views or positions of any entities they represent.