BGD e-GOV CIRT

বিজিডি ই-গভ সার্ট
বাংলাদেশ কম্পিউটার কাউন্সিল
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ
ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়
আইসিটি টাওয়ার, প্লট # ই-১৪/এক্স, আগারগাঁও, শেরে বাংলা নগর, ঢাকা-১২০৭

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

তারিখঃ ২৩ নভেম্বর ২০২৩

সাইবার নিরাপত্তা সংক্রান্ত সতর্কতা

বাংলাদেশের সাইবার স্পেসের সুরক্ষা নিশ্চিত করার লক্ষ্যে বাংলাদেশ সরকারের কম্পিউটার ইনসিডেন্ট রেসপন্স টিম (BGD e-GOV CIRT) সক্রিয়ভাবে গুরুত্বপূর্ণ থ্রেট ইনটেলিজেন্স সংক্রান্ত তথ্যাদি প্রকাশ করে থাকে। এরই ধারাবাহিকতায় সার্ট সাম্প্রতিককালে তথ্য পরিকাঠামোর জন্য ঝুঁকিপূর্ণ কিছু দুর্বলতা (critical vulnerabilities) চিহ্নিত করেছে। এরূপ ঝুঁকিপূর্ণ দুর্বলতাসমূহ ডিজিটাল অবকাঠামো হতে দূরিকরণের মাধ্যমে সম্ভাব্য সাইবার আক্রমন প্রতিহত করা যেতে পারে। চিহ্নিত শীর্ষ দুর্বলতাসমূহ সম্পর্কিত তথ্য নিম্নরূপ:

No.	CVE	Vendor	Affected product(s)	Type of vulnerability	Severity	CVSS score
1	CVE-2023-46747	F5 Networks	BIG-IP Configuration Utility	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	Critical	9.8
2	CVE-2023-46604	Apache	Apache ActiveMQ	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Critical	10
3	CVE-2023-36845	Juniper	Junos OS	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability. It is chained with (CVE-2023-36844 , CVE-2023-36846, CVE-2023-36847, CVE-2023-36851)	Critical	9.8
4	CVE-2023-4966	Citrix	NetScaler ADC and NetScaler Gateway	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Critical	9.4
5	CVE-2022-26134	Atlassian	All versions of Confluence Data Center and Server	Remote Code Execution	Critical	9.8
6	CVE-2023-22518	Atlassian	All versions of Confluence Data Center and Server	Atlassian Confluence Data Center and Server Improper Authorization Vulnerability	Critical	10
7	CVE-2023-22515	Atlassian	Publicly accessible Confluence Data Center and Server instances	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	Critical	10

সাইবার নিরাপত্তা বিষয়ক পরামর্শ:

- ক্রমবর্ধমান সাইবার হুমকি মোকাবেলায় সামগ্রিক সক্ষমতা বৃদ্ধি করা।
- ঝুঁকিপূর্ণ হুমকিসমূহ চিহ্নিতকরনে সক্রিয় উদ্যোগ নেয়া।
- উল্লেখিত সম্ভাব্য দুর্বলতার চিহ্নিতকরনে অগ্রাধিকার দেয়া।
- সচেতনতা বৃদ্ধির জন্য সকল ব্যবহারকারীদের সাইবার নিরাপত্তা প্রশিক্ষণকে অগ্রাধিকার দেয়া।
- সন্দেহজনক গতিবিধি উদঘাটনের জন্য বিগত ৬ (ছয়) মাসের নেটওয়ার্ক কমিউনেকেশন্স লগ পর্যবেক্ষন করা।
- সকল সিস্টেমে নিয়মিত Vulnerability Assessment and Penetration Testing (VAPT) পরিচালনা করা।
- ডিজিটাল অবকাঠামোতে সন্দেহজনক কার্যকলাপ বা দুর্বলতা পরিলক্ষিত হলে cirt@cirt.gov.bd ইমেইলের মাধ্যমে BGD e-GOV CIRT-কে অবহিত করা।