হার্টব্লিড | এক নতুন আতঙ্কের নাম

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

তথ্যপ্রযুক্তির এই যুগে আমাদের অনেক কাজ এখন হয় ইন্টারনেটের মাধ্যমে। তাই ইন্টারনেট আমাদের জীবনযাত্রাকে সহজতর করার পাশাপাশি সৃষ্টি করেছে অনেক ধরনের নতুন জটিলতা, যা আমাদের কমপিউটিং জীবনকে অনিরাপদ করে তুলছে। সম্প্রতি ইন্টারনেট ব্যবহারকারীদের জন্য নতুন হুমকি হয়ে দেখা দিয়েছে 'হার্টব্লিড' নামের এক বাগ। এই বাগের মাধ্যমে হ্যাকারেরা খুব সহজেই ব্যবহারকারীর যাবতীয় তথ্য, যেমন : ব্যক্তিগত তথ্য, ই-মেইল পাসওয়ার্ড, ক্রেডিট কার্ডের তথ্য ইত্যাদি চুরি করতে পারে। ইন্টারনেটে যখন দুটি কমপিউটার বা ডিভাইসের মধ্যে তথ্য দেয়া-নেয়া হয়, তখন তা বিশ্বের বিভিন্ন স্থানে বসানো রাউটার ঘুরে তার গন্তব্যে পৌঁছে। এখন যদি দু'টি ডিভাইসের (যেমন : স্মার্টফোন, কমপিউটার, ট্যাব ইত্যাদি) মধ্যে যে তথ্য দেয়া-নেয়া হচ্ছে, তা যদি স্বাভাবিক বা পেন টেক্সট আকারে হয়, তবে সোর্স থেকে ডেস্টিনেশনের মাঝখানে বসানো যেকোনো ডিভাইসে সেই তথ্য ক্যাপচার করে পড়ে ফেলতে পারে। যেমন : বাংলাদেশের কোনো একজন ক্রেতা অ্যামাজনডটকম নামে আমেরিকার ই-কমার্স সাইটে কোনো পণ্য কিনতে চায়, তবে সে তার নিজের ও তার ক্রেডিট কার্ডের তথ্য ইন্টারনেটের মাধ্যমে দেবে। বাংলাদেশ থেকে আমেরিকাতে অ্যামাজনডটকমের সার্ভারের মাঝখানে অনেক রাউটার ও নেটওয়ার্ক ডিভাইস ঘুরে সেই তথ্য সার্ভারে পৌঁছায়। এখন এই যাত্রাপথে কেউ যাতে তথ্য চুরি করে নিয়ে যেতে না পারে, তার জন্য এনক্রিপশন পদ্ধতি ব্যবহার করা হয়। পৃথিবীতে বিভিন্ন প্রটোকলের মধ্যে সবচেয়ে জনপ্রিয় হলো এইচটিটিপিএস। এই প্রটোকলটি এইচটিটিপি ও এসএসএল প্রটোকলের সমষ্টি। এসএসএলের ইমপ্লিমেনটেশনের মধ্যে সবচেয়ে জনপ্রিয় হলো ওপেনএসএসএল। হার্টব্লিড হলো সিকিউরিটি প্রোগ্রামিংয়ের একটি ত্রুটিমাত্র, যা বছর দুয়েক আগে জার্মান সফটওয়্যার ডেভেলপার রবিন সেগেলম্যানের ভুলে তৈরি হয়েছিল ওপেনএসএসএল প্রোগ্রামিংয়ের সময়। ২০১১ সালে ওপেনএসএসএলের জন্য সফটওয়্যার ত্রুটি সারানো ও নতুন ফিচার যুক্ত করার সময় দুর্ঘটনাবশত এই ত্রুটি থেকে যায়। সম্প্রতি নতুন একটি সিকিউরিটি হোল ধরা পড়েছে গুগলের বিশেষজ্ঞ নীল মেহতার চোখে।

হার্টব্লিড যেভাবে ক্ষতি করে

এটি মূলত ওপেন সোর্স ক্রিপটোগ্রাফি লাইব্রেরি ওপেনএসএসএলের একটি সফটওয়্যার বাগ বা ত্রুটি। এই সফটওয়্যারটি বেশিরভাগ ওয়েবসাইটে তথ্য নিরাপত্তার ক্ষেত্রে ব্যবহার করতে দেখা যায়। এসএসএল/টিএসএল এনক্রিপশন ইন্টারনেট নিরাপত্তায় ব্যবহার হলেও এই ত্রুটির কারণে তথ্য চুরি হওয়ার আশঙ্কা থেকে যায়। ওয়েব, মেইল, ইনস্ট্যান্ট মেসেজিং (আইএম), ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (ভিপিএন) প্রভৃতি অ্যাপ্লিকেশনের যোগাযোগ নিরাপত্তা ও প্রাইভেসির জন্য এসএসএল/টিএসএল ব্যবহার করা হয়। এই বাগ দুর্বৃত্তদের ইন্টারনেট ব্যবহার করে ওপেনএসএসএল সুরক্ষিত সিস্টেমের মেমরি পড়ার সুযোগ করে দেয়। চুরি যাওয়া পাসওয়ার্ড ও কী ব্যবহার করে হ্যাকারেরা অতীতের বা ভবিষ্যতের যেকোনো এনক্রিপটেড বা সুরক্ষিত তথ্যও দেখতে পারবে। এই ত্রুটির সুযোগ নিয়ে প্রতিবার এরা একটি সার্ভার থেকে ৬৪ কিলোবাইট পর্যন্ড় ডাটা চুরি করতে পারবে। তবে একই পদ্ধতিতে বারবার চেষ্টা চালিয়ে হাতিয়ে নেয়া যাবে অসংখ্য ব্যবহারকারীর তথ্য। সাইবার নিরাপত্তা বিশ্লেষক প্রতিষ্ঠান ফক্স-আইটি তাদের ওয়েবসাইটে জানিয়েছে, বর্তমানে যত ওয়েবসাইট আছে, তার অর্ধেকই তথ্যের নিরাপত্তার জন্য ওপেনএসএসএল এনক্রিপশন ব্যবহার করে। অবশ্য হার্টব্লিড বাগ পাওয়া গেছে দুই বছর আগে বাজারে ছাড়া ওপেনএসএসএলের একটি সংস্করণে। ব্যবহারকারীদের জন্য প্রতিষ্ঠানটি সতর্কতা জারি করেছে এবং ওপেন এসএসএলের নতুন সংস্করণ ব্যবহারের পরামর্শ দিয়েছে।

যেসব সাইট বেশি হুমকিতে আছে

হার্টব্লিড ঝুঁকিতে আছে এবং নিরাপদ থাকার জন্য পাসওয়ার্ড বদলে নেয়া প্রয়োজন এমন সাইটগুলোর তালিকাও প্রকাশ করেছে প্রযুক্তিবিষয়ক সাইট ম্যাশএবল। ম্যাশএবলের প্রতিবেদন অনুযায়ী– ফেসবুক ইনস্ট্যাগ্রাম, পিন্টারেস্ট আর টাম্বলারের পাসওয়ার্ড পাল্টে নেয়া প্রয়োজন। সবগুলো সোশ্যাল মিডিয়াভিত্তিক প্রতিষ্ঠানেরই একই দাবি, হার্টব্লিড দুর্বলতা থাকলেও ফাঁস হয়নি কোনো গোপন ডাটা। হার্টব্লিড আবিষ্কারের সাথে সাথেই বাগটি ঠিক করতে প্রয়োজনীয় পদক্ষেপ নেয়ার দাবিও করেছে প্রতিষ্ঠানগুলো। এরপরও ব্যক্তিগত ডাটার নিরাপত্তার স্বার্থে পাসওয়ার্ড বদলে নেয়াই শ্রেয় বলে জানিয়েছে ম্যাশএবল।

হার্টব্লিড হুমকিতে আছে শীর্ষ দুই সার্চ জায়ান্ট গুগল আর ইয়াহুও। হার্টব্লিড বাগের উপস্থিতি ছিল জি-মেইল আর ইয়াহু মেইলের সার্ভারেও। দুটি প্রতিষ্ঠানের সফটওয়্যার প্যাচের মাধ্যমে বাগটি ঠিক করে ফেলার কথা বলা হয়েছে। তারপরও রয়ে গেছে সফটওয়্যার প্যাচ করার আগেই ব্যবহারকারীদের ব্যক্তিগত তথ্য আর পাসওয়ার্ড বেহাত হওয়ার আশঙ্কা। তাই গুগল আর ইয়াহু বিভিন্ন সার্ভিসের পাসওয়ার্ড পাল্টে নেয়াই হবে ইতিবাচক।

ই-কমার্সভিত্তিক সাইটগুলোর মধ্যে ঝুঁকিতে আছে অ্যামাজন, গোড্যাডি আর ইটসি। সফটওয়্যার আপডেট করেছে এদের সবাই। তবে ঝুঁকিতে আছে শীর্ষ ফটো, ভিডিও এবং গেমিং সাইটগুলোর মধ্যে অনেকগুলোই। ফ্লিকার, হুলু, মাইনক্রাফট, নেটফ্লিক্স, ইউটিউব এবং সাউন্ডক্লাউড এসব সাইটের সার্ভারেই ব্যবহার করা হতো ওপেনএসএসএল প্যাকেজ। এই সাইটগুলোর পাসওয়ার্ডও পাল্টে নেয়া প্রয়োজন।

সব খানেই হার্টব্লিড

প্রযুক্তি-প্রতিষ্ঠান সিসকো ও জুনিপার সম্প্রতি দুই ডজনেরও বেশি নেটওয়ার্কিং যন্ত্রে হার্টব্লিডের আক্রমণ শনাক্ত করেছে। সার্ভার, রাউটার, সুইচ, মোবাইল ফোন, ভিডিও ক্যামেরাসহ নানা ধরনের প্রযুক্তিপণ্য এই আক্রমণের শিকার হয়েছে। অন্যান্য যন্ত্রও এই হার্টব্লিড বাগের শিকার হয়েছে কি না, তা নিয়েও পরীক্ষা করছেন প্রযুক্তি গবেষকেরা। এদিকে হার্টব্লিড ঝুঁকিতে আছেন বিশ্বব্যাপী কয়েক কোটি অ্যান্ড্রয়িড ডিভাইস ব্যবহারকারী। গুগলের ঘোষণা অনুযায়ী, হার্টব্লিড ঝুঁকিতে আছেন অ্যান্ড্রয়িড ৪.১.১ জেলি বিন অপারেটিং সিস্টেম ব্যবহারকারীরা। ৪.১.১ জেলি বিন ব্যবহারকারীদের সঠিক সংখ্যা না জানা গেলেও বিশ্বব্যাপী লাখ লাখ অ্যান্ড্রয়িড ডিভাইসে অপারেটিং সিস্টেমটি ব্যবহার করা হচ্ছে।

নিরাপদ থাকতে করণীয়

০১. পাসওয়ার্ড পরিবর্তন করুন। তবে পাসওয়ার্ড পরিবর্তন করলেও ঝুঁকি একেবারে শেষ হয়ে যাবে না। ওয়েবসাইটের নিরাপত্তা প্যাচ উন্মুক্ত হওয়ার পর পাসওয়ার্ড পরিবর্তন কাজে লাগবে। এখন পাসওয়ার্ড পরিবর্তন করলে এক সপ্তাহ পর আবারও তা পরিবর্তন করে দিতে পারেন।

০২. আপনি যেসব ওয়েবসাইটে ব্রাউজ করছেন সেগুলো নিয়ে চিন্ড়িত? ফায়ারফক্স ব্রাউজারে একটি ফ্রি অ্যাড-অন রয়েছে, যা রং পরিবর্তনের মাধ্যমে আপনার ব্রাউজ করা সাইটটি নিরাপদ কি না জানিয়ে দিতে পারে। অ্যাড-অন ডাউনলোড করার লিঙ্ক (addons.mozilla.org/en-US/firefox/addon/heartbleed-checker/)

০৩. আপনার রাউটার বা ব্যবহার হওয়া যন্ত্রপাতিগুলোর ওয়েবসাইট পরীক্ষা করে দেখুন। এসব প্রতিষ্ঠান তাদের সাইটে হার্টব্লিডের সমস্যায় আক্রান্ড় কি না সে তথ্য দিতে পারে বা সমাধান রাখতে পারে। ইন্টারনেট থেকে অজানা কোনো সফটওয়্যার আপডেট কিংবা কোনো কিছু ডাউনলোড ও ইনস্টল করার বিষয়ে সতর্ক থাকুন।

তবে সর্বশেষ কথা হলো, হার্টব্লিড নিয়ে বেশি আতঙ্কিত হওয়ারও তেমন কোনো কারণ নেই। যদি আমরা যথাযথ নিরাপত্তামূলক ব্যবস্থা নিই, তবে হার্টব্লিডের আক্রমণ থেকে নিজেদেরকে নিরাপদ রাখতে পারব।

আরও জানতে

হার্টবিড সম্পর্কে বিস্ড়ারিত জানতে যেতে পারেন হার্টব্লিড বাগ (heartbleed.com) সাইটে কজ

ফিডব্যাক : jabedmorshed@yahoo.com