What is a Teardrop Attack?

In a denial-of-service (DoS) **teardrop attack**, a client sends a malformed information packet to a machine and exploits the error that occurs when the packet is reassembled resulting in degraded server performance.

What is a teardrop attack?

A teardrop attack is a type of denial-of-service (DoS) attack (an attack that attempts to make a computer resource unavailable by flooding a network or server with requests and data.) The attacker sends fragmented packets to the target server, and in some cases where there's a TCP/IP vulnerability, the server is unable to reassemble the packet, causing overload.

How does a teardrop attack work?

TCP/IP implementations differ slightly from platform to platform. Some operating systems—especially older versions of Windows and Linux— contain a TCP/IP fragmentation reassembly bug. Teardrop attacks are designed to exploit this weakness.

In a teardrop attack, the client sends an intentionally fragmented information packet to a target device. Since the packets overlap, an error occurs when the device tries to reassemble the packet. The attack takes advantage of that error to cause a fatal crash in the operating system or application that handles the packet.

Why are teardrop attacks important?

Many organizations still rely on older, obsolete, or unpatched operating systems to run legacy applications that they still need. Such organizations are vulnerable to teardrop attacks that threaten to take down mission-critical applications.

How to prevent teardrop attack?

You can prevent teardrop attack in general by following the method given below.

Protecting the network layer:

These attacks target network layer, so your system must defend it at all cost. You can use proper firewall network which filters junk data.

Using caching serves:

caching servers are very useful mitigating tool to prevent teardrop attack. These servers can provide static content so that the website can run.

Using secured proxy:

This method involves inspecting incoming packets for the violation of data fragmentation rule which prevents bug-laden data coming to your device.

That's all for today, we hope that this article help you to understand more about this attack and ways to prevent it. Let us know if you have any queries and suggestion for us via comment section.