Windows vulnerability

Technology, Information Technology

Vulnerability Report The TLS Protocol CBC Mode Information Disclosure Vulnerability is found on a variation of windows operating systems. This bug allows an attacker to gain remote access to the target systems, meaning that they have unauthorized and uncontrolled access to an organization’s sensitive information. This is, primarily, due to the fact that design flaws exist when using the cipher-block chaining (CBC) approach of operation within the encryption protocols used at the transport layer. It is in this way that malicious attackers could lure system users to websites that contain malicious code, upon which, requests will be processed allowing them access to the target systems. This report highlights the details of attacks conducted using this vulnerability, the systems that are vulnerable to this attack, the consequences and effects of the attacks, document some cases where such attacks have taken place and finally explore the fixes that exist so far.

How it Works

As stated above, such an attack takes advantage of the design flaws in transport layer, such that the attacker is able to intercept secure traffic from the target computer. In this way, the attacker could make use of an enticing website to attract a user within the organization. Any processing handled on that website, could trigger sensitive information to flow to the attackers website. A successful attack would be possible if the attacker is able to decrypt the traffic from the target systems, which is normally encrypted.

Affected Systems

The systems using the following operating systems are characterized as vulnerable. They include (Security Focus):

Windows XP service pack 3

Windows 7 professional

However, the vulnerability will not be extended to users of SharePoint 2010 and Microsoft internet information services (IIS7). These systems will function normally with no fear of remote attacks unless they are deployed on machines with the above named operating systems.

Impact of this Vulnerability

The uncontrolled and unauthorized access to target systems creates a channel that the attacker can use to acquire the organization’s sensitive data or plan future attacks. This means, sensitive information could be leaked to competitors; thus, diminishing any competitive advantages that may have existed.

Reported Cases

Currently, there are no reported cases of attacks conducted by exploiting this vulnerability. According to a vulnerability alert, this exploit has been unproven (Cisco). However, this does not belittle the fact that the vulnerability still exists and measures should be taken to ensure that the organization’s data is safe.

Recommendations and Fixes

Given the fact that this vulnerability can be exploited through remote means, it is important to ensure that the filters and checks are put in place to control access to the organization’s data. Computers with operating systems that are vulnerable should only have access to trusted networks and computers within the organization (Symantec). It is also prudent to make use of Network Intrusion Detection Systems (NIDS), which will be instrumental in analyzing the traffic (Cisco). Such systems will be able to identify, suspicious activity that may happen to be attempts to exploit the systems. Microsoft has also provided updates that can be deployed automatically to all computers within the organization. Cisco advocates for the use of RC4 algorithm instead of CBC for encryption; however, in such a case all systems that are in communication will be required to support this algorithm (Cisco). Aside from these solutions provided, the organization and its users also have a role to play. Administrators should only give access to company systems to trusted users, they should also regularly monitor systems that are vulnerable, and finally, users should not open suspicious emails or emails that originate from unknown sources.

Works Cited

Cisco. “ Microsoft Windows TLS Protocol Information Disclosure Vulnerability.” Cisco. n. p. 10 July 2012. Web. 15 Oct. 2012.

Security Focus. “ Microsoft Windows TLS Protocol CBC Mode Information Disclosure Vulnerability.” Security Focus. n. p. 10 July 2012. Web. 15 Oct. 2012.

Symantec. “ Microsoft Windows TLS Protocol CBC Mode Information Disclosure Vulnerability.” Symantec. n. p. 10 July 2012. Web. 15 Oct. 2012.