Developments in hacking, cybercrime, and malware

Technology, Development

The attacker can then execute malicious tiles installed by the initial security weakness. Also, an attacker can exploit this vulnerability by enticing a victim to open a malicious Web page. A successful attack will allow an attacker to execute remote code on a victims computer, This vulnerability may be appealing to attackers because, rather than relying on a plug-in that may or may not be installed on a target computer; it relies only on the use of a version of a popular browser, thereby increasing the number of potential victims.

Cisco response to MAD collisions In certificates Issued by vulnerable certificate authorities Is Its release of the Cisco Adaptive Security Appliance (AS) and ISO may tooth serve as certificate authorities and by default use the MAD hashing algorithm In the digital signatures of certificates issued to end users and devices The hashing algorithm used In digital certificates on the Cisco AS cannot be changed; however, the AS Is unlikely to be affected by the attacks described In this research due to the way certificates are generated on the device.

Cisco recognizes the weaknesses in MAD and plans to alter the signature algorithm used in digital certificates and modify the methods utilized in creation of CA and endpoint certificates.