ASA BEAST-betrouwbaarheidsoplossingen

Inhoud

Inleiding

Dit document beschrijft een kwetsbaarheid binnen de software van Cisco adaptieve security applicatie (ASA) die onbevoegden toegang geeft tot beschermde inhoud. Hierin worden ook de zorgpunten beschreven.

Probleem

De kwetsbaarheid van browser Exploit Against SSL/TLS (BEAST) wordt door een aanvaller benut om beschermde inhoud effectief te lezen via Initialization Experience (IV) ketting in Cipher Block Chaining (CBC) encryptie mode met een bekende ruimtetoestand.

De aanval gebruikt een gereedschap dat een kwetsbaarheid exploiteert in het algemeen gebruikte protocol van de Veiligheid van de Vervoerslaag 1 (TLSv1). De kwestie is niet geworteld in het protocol zelf, maar in de formules die het gebruikt. Het TLSv1 en Secure Socket Layer versie 3 (SSLv3) begunstigen CBC-ciphers, waar de aanval van het opvulkanaal plaatsvindt.

Gebruikershandeling

Zoals aangegeven door het SSL Pulse SSL-implementatieonderzoek, dat is opgezet door de Trustworth Internet Movement, zijn meer dan 75% van de SSL-servers vatbaar voor deze kwetsbaarheid. De logistiek van het BEAST-instrument is echter vrij ingewikkeld. Om BEAST te kunnen gebruiken om het verkeer af te luisteren moet een aanvaller in staat zijn om pakketten heel snel te lezen en te injecteren. Dit kan de effectieve doelen voor een BEAST-aanval beperken. Bijvoorbeeld, een beAST-aanvaller kan effectief willekeurig verkeer grijpen op een WIFI-hotspot of waar al het internetverkeer gebotteld is door een beperkt aantal netwerkgateways.

Oplossing

BEAST maakt gebruik van de zwakte van het in het protocol gebruikte algoritme. Aangezien deze functie van invloed is op het CBC-algoritme, was de oorspronkelijke werkwijze voor dit onderwerp

om in plaats daarvan naar het RC4-algoritme te switches. De zwakheden van het Key Scheduling-algoritme van het RC4-artikel dat in 2013 werd gepubliceerd, onthullen echter dat zelfs RC4 een zwakte had die dit ongeschikt maakte.

Om aan dit probleem te kunnen werken, heeft Cisco deze twee oplossingen voor de ASA geïmplementeerd:

- Cisco bug-ID CSCts83720: *upgrade naar TLS 1.1/1.2*

  Upgradeffiti en gebruik TLS 1.1/1.2. De beperking met deze oplossing is dat deze alleen van toepassing is op ASA 5500-X ASA-platforms. De versleutelingshardware op bestaande ASA-platforms (ASA 5505 en de ASA 5500-reeks) ondersteunt TLSv1.2 niet. Als gevolg daarvan is een oplossing voor deze platforms niet haalbaar.

  Vanwege protocolbeperkingen is er geen oplossing voor SSLv3 of TLSv1.0; de meeste moderne browsers hebben echter verschillende manieren van mitigatie toegepast .

- Cisco bug-ID CSCuc85781: *WebexVPN-calibratie*

  Voor de ASA-softwareversies die TLSv1.2 niet ondersteunen, maakte Cisco de koekjes willekeurig met deze oplossing om het risico te verminderen. Dit voorkomt BEAST-aanvallen niet volledig, maar helpt ze wel te verzachten.

  Tip: De enige manier om volledig beschermd te worden tegen de kwetsbaarheid van het BEAST is om TLSv1.2 te gebruiken. Dit lijkt op cifen. Cisco blijft nieuwere, sterkere ciphers in nieuwere code toevoegen, en oudere ciphers kunnen bekende kwesties (zoals RC4) hebben. Dus, raadt Cisco u aan om naar de nieuwere protocollen en cifen te bewegen.