SSDP

Das Simple Service Discovery Protocol (SSDP) ist ein Netzwerkprotokoll, welches zur Suche nach UPnP-Geräten im Netzwerk dient. SSDP nutzt üblicherweise den Port 1900/udp. Systeme, die SSDP-Anfragen aus dem Internet beantworten, können zur Durchführung von DDoS-Reflection/Amplification-Angriffen missbraucht werden. Dabei werden UDP-Antworten auf gespoofte M-SEARCH-Anfragen generiert, die von dem angegriffenen Opfer zu kommen scheinen.

Wir haben Beschwerden erhalten, dass die hier aufgeführten Systeme an einem großräumigen DDoS-Reflection/Amplification-Angriff teilgenommen haben. Bitte sichern Sie Ihre Systeme schnellstmöglich durch eine der folgenden Maßnahmen ab:

- Blockieren Sie an Ihrer Firewall den externen Zugriff auf Port 1900 (udp).
- Deaktivieren Sie UPnP (SSDP ist eine Komponente des UPnP-Subsystems und kann nicht separat deaktiviert werden).
- Konfigurieren Sie das Gerät so, dass es nicht auf externe M-SEARCH-Anfragen antwortet oder beschränken Sie die Anzahl der Antworten.

Referenzen

[1] Wikipedia: Simple Service Discovery Protocol [1]
[2] Sucuri: Quick Analysis of a DDoS Attack Using SSDP [2]
[3] US-CERT: UDP-based Amplification Attacks [3]
[4] Shadowserver: Open SSDP Scanning Project [4]

Links

[1] http://de.wikipedia.org/wiki/Simple_Service_Discovery_Protocol
[2] http://blog.sucuri.net/2014/09/quick-analysis-of-a-ddos-attack-using-ssdp.html
[3] https://www.us-cert.gov/ncas/alerts/TA14-017A
[4] https://scan.shadowserver.org/ssdp/

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/ssdp/