softScheck
we identify vulnerabilities others don't

SNMP-Fuzzer erfolgreich an PLC S7-1200 getestet

Prof. Dr. Hartmut Pohl, Valeri Milke, B.Sc.

Sankt Augustin 21. Januar 2013

Viele Hersteller für Speicherprogrammierbare Steuerungen (SPS) implementieren in ihren Produkten einen SNMP-Dienst zur Überwachung und Konfiguration. Aufgrund der Einfachheit des Protokolls werden meist veraltete Versionen verwendet, die besonders in der Default-Konfiguration viele kritische Sicherheitslücken enthalten. SNMP-Fuzzer wurde im Rahmen einer Untersuchung von SPS / PLC als Metasploit Modul entwickelt. Das Modul ermöglicht die Identifizierung von Sicherheitslücken durch die dynamische Methode Fuzzing in einer SNMP-Implementierung.

Die Entwicklung des SNMP-Protokolls reicht zurück bis 1987 mit dem SNMP-Vorgänger SGMP (Simple Gateway Monitoring Protocol). 1990 wurde darauf basierend das Netzwerkverwaltungsprotokoll SNMP (Simple Network Management Protocol) in Version 1 und 2 entwickelt und wird seitdem zur Überwachung und Konfiguration von Geräten (z.B. Drucker, Server) über das Netzwerk verwendet. Die Versionen bieten nur einfache Sicherheitsmechanismen, die von Angreifern problemlos umgangen werden können (z.B. durch „Community-Names"). Erst Version 3 wurde um Sicherheitsmechanismen wie Authentifizierung und Verschlüsselung erweitert, mit denen ein - nach dem heutigen Stand - angemessenes Sicherheitsniveau erreichbar ist. Aufgrund des hohen Implementierungsaufwands und gegenwärtig geringer Verbreitung mit einhergehender Inkompatibilität, bevorzugen viele Hersteller die unsichere Version 2 oder sogar Version 1.

Die SNMP-Kommunikation findet zwischen den zwei Teilnehmern „Manager" und „Agent" auf den UDP-Ports 161 und 162 statt. Der Agent befindet sich auf dem Gerät, das überwacht oder konfiguriert werden soll. Der Manager konfiguriert oder überwacht das Zielgerät über SNMP-Befehle. Mit Hilfe von „SNMP-Get" und einer SNMP-Objekt-ID (OID) kann der Manager eine Anfrage an den Agenten schicken, um den Objektinhalt abzufragen. Dieser antwortet mit „SNMP-Response", welche alle Attribute des Objekts, wie Datentyp, Wert, Name wiedergibt. „SNMP-Get"-Anfragen dienen somit der reinen Überwachung. Durch den „SNMP-Set"-Befehl können die ausgelesenen Werte geändert werden, sofern eine Schreibberechtigung existiert.

In der Version 1 und 2 existiert nur eine einfache Form der Zugriffsberechtigung. Es wird mit einer „SNMP-Get"- oder „SNMP-Set"- Anfrage ein „Community-Name" mitgeschickt, der entweder über eine „read-only" oder eine „read-write" Berechtigung verfügt. Da die Community in Version 1 in Klartext gesendet wird, kann mit einem Netzwerk-Sniffer die Übertragung einfach mitgeschnitten werden. Version 2 verschlüsselt zwar die Communities, jedoch belassen viele Hersteller die Default-Communities „public" für „read-only" und „private" für „read-write". Zusätzlich lassen sich durch Brute-Force- oder Library-Angriffe häufig „Community-Names" mit Lese- und/oder Schreibrechten herausfinden, wodurch Informationen über SNMP-fähige Geräte ausgelesen und Konfigurationen manipuliert werden können.

SNMP-Fuzzer nutzt die Schreibberechtigung auf Objekte, um eine zufällige und mit hoher Wahrscheinlichkeit fehlerhafte Konfiguration vorzunehmen und somit fehlerhaftes Verhalten bei der Zielsoftware zu provozieren. SNMP-Fuzzer sendet pro Sekunde mehrere invalide Konfigurationsanfragen. Die Geschwindigkeit hängt von der Latenzzeit des Netzwerks ab. Durch Tests konnten mit SNMP-Fuzzer diverse Sicherheitslücken identifiziert werden, die sich in Form von Denial of Service-Angriffen ausnutzen lassen. Der SNMP-Fuzzer benötigt die IP-Adresse des Zielgeräts, eine Community mit „read-write"-Berechtigung, die OID und den Datentyp, damit der Fuzzer nur dem Objekt angepasste Fuzzdaten generiert. Community-Names mit „read-write"-Berechtigung können von Vulnerability Scannern wie Nessus oder OpenVAS identifiziert werden. Alternativ ermöglicht das Tool ADMsnmp, Objekte mit „read-write"-Berechtigung in Communities zu identifizieren. Mit dem Tool MIB Browser lassen sich alle Objekte mit den zugehörigen OIDs auflisten und alle Attribute anzeigen, die für den Fuzzer benötigt werden.

Wird das Metasploit-Modul ausgeführt, wird eine laufende Instanz (bei Metasploit als „Job" bezeichnet) erzeugt. Ein SNMP-Fuzzer-Job fuzzt gleichzeitig immer nur ein SNMP-Objekt, da für jedes Objekt sein individueller Datentyp als Parameter übergeben wird. Das Metasploit-Framework unterstützt eine parallele Bearbeitung von mehreren Jobs, somit ist es möglich, viele Objekte gleichzeitig zu fuzzen. Der parallele Einsatz von SNMP-Fuzzer wird empfohlen, um zum einen die Fuzzing-Geschwindigkeit und damit die Effizienz zu erhöhen, zum anderen kann es auch zur höheren Effektivität führen, da einige Fehler erst in Kombination aus fehlerhaft konfigurierten Objekten zur Identifizierung von Sicherheitslücken führen.

SNMP-Fuzzer eignet sich für alle Produkte, bei denen SNMP in der Version 1 oder Version 2 implementiert ist.

Erstmals wurde damit ein SNMP-Fuzzer entwickelt, der Objekte gezielt unter Beibehaltung des jeweiligen Datentyps manipuliert und nicht nur zufällige Anfragen sendet.

Der Fuzzer wurde erfolgreich an der Siemens PLC S7-1200 getestet. http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-724606.pdf

Die Veröffentlichung des Fuzzer erfolgt zeitnah nach Patchen der Sicherheitslücke.