VULNERABILITY SUMMARY FOR CVE-2013-1673

Term paper in Computer Security

By:

Kea Mei

TARTU
2014
CONTENTS

OVERVIEW OF VULNERABILITY CVE-2014-1673 ................................................................. 3
  About the Check Point Session Authentication Agent .................................................... 3
  Detailed Description of the Issue .................................................................................. 3
SOLUTIONS ...................................................................................................................... 5
REFERENCES ................................................................................................................ 6
OVERVIEW OF VULNERABILITY CVE-2014-1673

Common Vulnerabilities and Exposures (CVE) database includes the vulnerability, named CVE-2014-1673, which states that Check Point Session Authentication Agent allows remote attackers to obtain sensitive information (user credentials) via unspecified vectors \(^1\).

Encrypted communication between agent and security gateway has been introduced due to several issues which were revealed in the previous versions (4.0 and lower) of the product. Research showed that it is still (in versions 4.1 and higher) possible to exploit previously known vulnerabilities - gateway impersonation and credential stealing - even though communication between agent and security gateway is using SSL (Secure Sockets Layer network protocol).

About the Check Point Session Authentication Agent

Check Point Session Authentication Agent is a service that is installed on endpoint system in order to communicate with security gateway and allow it to request and obtain user's credentials. Session Authentication is a part of Legacy Authentication suite which provides different authentication methods to allow or deny access to network resources.

R76 Security Gateway Technical Administration Guide \(^2\) defines typical Session Authentication operation in the following way:

1. The user initiates a connection directly to the server
2. The Security Gateway intercepts the connection
3. The Session Authentication agent challenges the user for authentication data and returns this information to the gateway
4. If the authentication is successful, the Security Gateway allows the connection to pass through the gateway and continue to the target server.

Detailed Description of the Issue

Check Point Security Gateway contains a flaw in the Session Authentication agent (version 4.1 and higher), which is caused by the lack of peer authentication in SSL communication.
This issue is caused by the system that allows the agent to specify a weak SSL cipher (which utilizes Secure Sockets Layer network protocol). Once the user is connected, essentially bypassing authentication to a degree, the system will return user credentials when prompted.[3]

Communication between Session Authentication agent and security gateway is performed using proprietary protocol. Since version 4.1 this communication scheme uses SSL as an underlying protocol to enable encryption of both protocol commands and user provided data. When SSL communication is negotiated between the gateway and agent, the following cipher suites are showed as if they are supported by the Session Authentication Agent:

- TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- TLS_DH_anon_WITH_RC4_128_MD5
- TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- TLS_DH_anon_WITH_DES_CBC_SHA
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

The TLS protocol RFC2246 [4] refers to above listed cipher suites: "The following cipher suites are used for completely anonymous Diffie-Hellman communications in which neither party is authenticated. Note that this mode is vulnerable to man-in-the-middle attacks and is therefore deprecated."

Taking into account above information, Check Point Session Authentication Agent is vulnerable to user credentials disclosure due the presence of weak encryption. It is possible to connect to Session Authentication Agent from attacker's machine, initiate SSL-based communication, pass SSL handshake without being authenticated and use encrypted channel to control agent (for example prompt user for login and password). The attack is possible from within the internal network. Unfortunatelly, all versions of Check Point Session Authentication Agent are vulnerable.
SOLUTIONS

For the attack to be successful, the attacker's machine must be allowed to connect to the end user (client) machine, on which Check Point Session Authentication Agent is running.

Proper configuration requires the user to define on his computer the IP address of the Security Gateway, which is allowed to issue authentication requests to Session Authentication Agent running on the client machine.

According to Check Point response to the Session Authentication Agent vulnerability [5], spoofing the Gateway IP address is not enough in this case, but this would reduce the possibility of the attack, because the attacker must complete a TCP handshake with the client's machine. It is safer, because there are 3 messages transmitted by TCP to negotiate and start a TCP session between two computers. The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network TCP socket connection before transmitting data such as SSH and HTTP web browser requests. Firstly, host A sends a TCP synchronized packet to host B, who then receives it. Then, host B sends a synchronized-acknowledgment and host A receives this. Thirdly, host A sends acknowledge and B receives it. Only then the TCP socket connection is established [6].

Session Authentication Agent feature will be end-of-life in the next major release of 2014. Check Point has advised costumers to use new Identity Awareness Software Blade instead [7].

Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.

Benefits of this are that Check Point Identity Awareness Software Blade increases visibility of user activities and prevents unauthorized access, while allowing users work remotely. It also prevents threats and data loss by restricting access to resources by users and devices.
REFERENCES


