Automation Theory

Connectwise Automate Security Scanner Results Guide

Properly securing an RMM is a complex task. This guide walks through the results of the Automate Security Scanner to provide a robust reference for the various risks and controls.

Server Ports

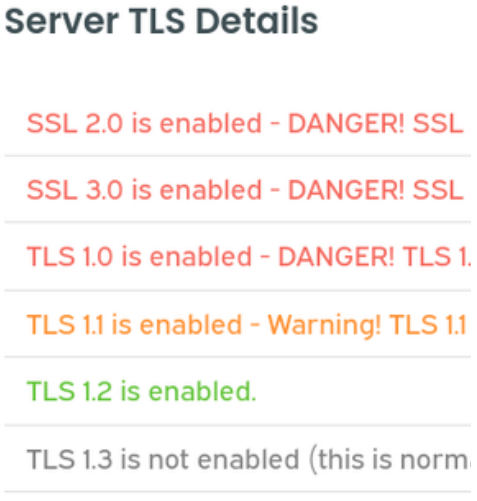
The required ports to run Automate have changed over the years, as have certain best practices. In a modern Automate stack, only ports 443/TCP and 75/UDP are required to be open to the outside world.

Port	Best Practice	Explanation
80/TCP	Closed	Plain-text communication should be disabled, as support for encryption is well established, and agent communication will function through most certificate issues by default.
443/TCP	Open	Encrypted communications should be the only option for Automate, and this should be the only open TCP port in a modern Automate deployment.
3306/TCP	Closed	MySQL access should be internal only.
12413/TCP	Closed	The CWA File Service should only be accessible internally.

TLS Versions and Ciphers

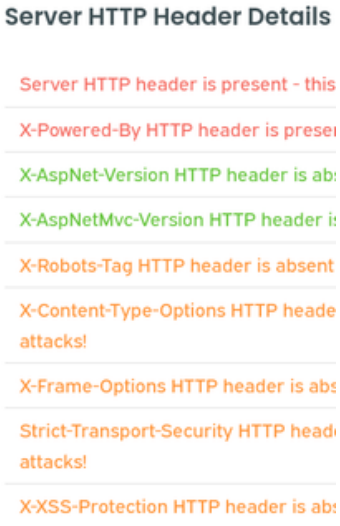
Transport Layer Security (TLS) versions 1.0 and 1.1 are considered less secure compared to more recent versions of TLS, such as TLS 1.2 and TLS 1.3. These older versions of TLS contain vulnerabilities that attackers can exploit. For example, attackers could intercept and read sensitive information, such as login credentials, making old versions of TLS inadvisable for use in secure environments.

We recommend using a reverse proxy for TLS hardening to mitigate these risks. A reverse proxy performs TLS offloading, ensuring inbound connections use strong and secure ciphers and protocol versions. This can help reduce the risk of eavesdropping and man-in-the-middle attacks that attempt to intercept or modify sensitive information in transit.



https://autothry.co/scan

Server HTTP Headers

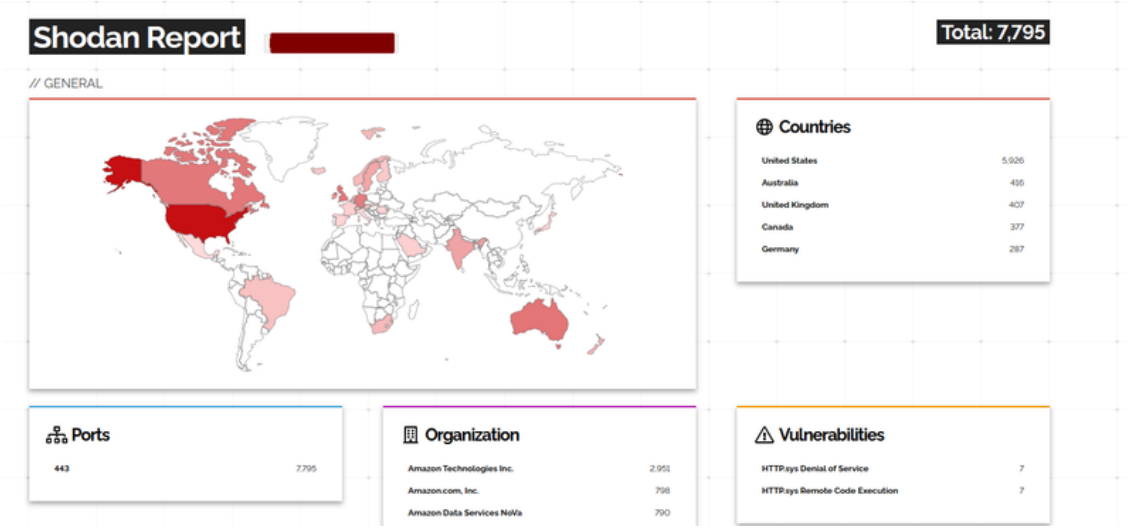


Header data in ConnectWise Automate can pose a security risk if not properly managed. Server-side headers provide information about the web server software and its version. This information can be used by attackers to identify potential vulnerabilities in the server software and to develop targeted attacks.

Missing security headers can also pose a risk. These headers provide additional security controls that help to protect web applications and their users from various types of attacks. Headers can protect against information stealing via cross-site scripting (XSS) attacks and content-type confusion, which exploits vulnerabilities in browsers and applications.

Automate administrators can configure a reverse proxy to add missing HTTP headers to requests before forwarding them to the requestor. Additionally, the proxy can remove or modify server-side HTTP headers to reduce the information disclosed about the web server.

Server Enumeration



Enumeration is the first step in a cyber attack as reconnaissance occurs. In the event of a zero-day vulnerability, threat actors will likely attempt to exploit any enumerable server, so preventing enumeration can be an extremely valuable security layer.

GeoIP restrictions are a basic least-access protection that can go a long way. By only allowing traffic from countries where clients reside, the attack surface is reduced significantly from the default configuration.

Search engine enumeration is the process of using search engines to locate specific software running on Internet-connected systems. Attackers can use search engine enumeration to identify potential targets and gather information about the servers, including the FQDN and the patch level of the application.

Shodan enumeration is a common issue for Automate servers but should be treated seriously. An attacker can use Shodan to search for Automate servers exposed to the Internet. Shodan can provide information about the IP addresses, operating systems, and services running on these servers, which an attacker can use to identify potential vulnerabilities and plan an attack. If an attacker discovers a zero-day vulnerability, they can use Shodan to find servers to exploit.