VersaMem, Software S1154 | MITRE ATT&CK®

Archived: 2026-04-05 16:51:43 UTC

Domain	ID		Name	Use
Enterprise	T1059		Command and Scripting Interpreter	VersaMem was delivered as a Java Archive (JAR) that runs by attaching itself to the Apache Tomcat Java servlet and web server.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	VersaMem staged captured credentials locally at `/tmp/.temp.data`.[1]
Enterprise	T1203		Exploitation for Client Execution	VersaMem was installed through exploitation of CVE-2024-39717 in Versa Director servers.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	VersaMem deleted files related to initial installation such as temporary files related to the PID of the main web process.[1]
Enterprise	T1056	.004	Input Capture: Credential API Hooking	VersaMem hooked and overrided Versa's built-in authentication method, `setUserPassword`, to intercept plaintext credentials when submitted to the server.[1]
Enterprise	T1040		Network Sniffing	VersaMem hooked the Catalina application filter chain `doFilter` on compromised systems to monitor all inbound requests to the local Tomcat web server, inspecting them for parameters like passwords and follow-on Java modules.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	VersaMem encrypted captured credentials with AES then Base64 encoded them before writing to local storage.[1]

Domain	ID	Name	Use
Enterprise	T1129	Shared Modules	VersaMem relied on the Java Instrumentation API and Javassist to dynamically modify Java code existing in memory.[1]

Source: https://attack.mitre.org/software/S1154