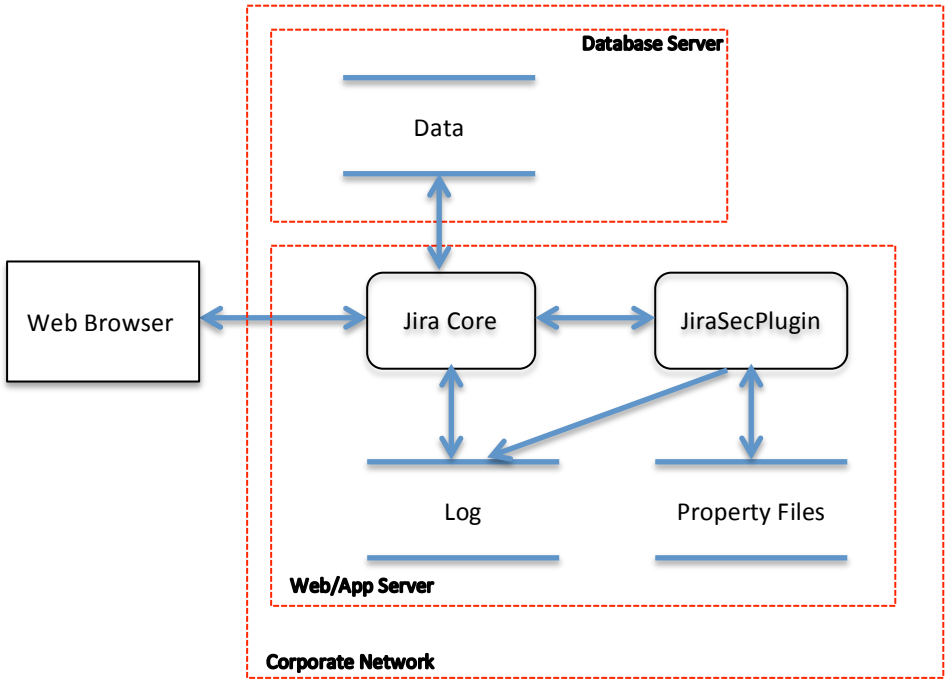
Threat Model and Attack Surface Analysis for JiraSecPlugin

This is important because the JiraSecPlugin will run with the admin privileges. Therefore, a compromise might have serious consequences to the organization.



Identification (STRIDE), Analysis & Mitigations

Threat	Element	Description	Mitigation
Spoofing	JiraSecPlugin	Insecure access permissions on a local directory allow a local attacker to plant a malicious binary in a trusted location. (A typical example is an application installer not properly configuring permissions on directories used to store application files.)-owasp	Custom directory is different from installation directory Custom directory is protected from unauthorized access
Tampering	JiraSecPlugin	It is possible for a malicious person to hide malware in a cloned version	Digital signature
	Property Files	Unauthorized access to property files	Custom directory is protected from unauthorized access
Repudiation	-	-	-
Information Disclosure	Property Files	Unauthorized access to property files	Custom directory is protected from unauthorized access
Denial-of-service	JiraSecPlugin	Bad inputs	Custom directory is protected from unauthorized access. Inputs are validated before use
Elevation of Privilege	-	-	-

New Attack Surface (Entry points)

Entry points	Description	Threats	Mitigations	Likelihood
3 Custom fields	JiraSecPlugin reads input from and sends output to the custom fields through the JIRA-API	Injection (xss, sql, etc)	Relies on input validation mechanism in JIRA. Input from config files are validated against bounded data in Jira.	Trivial - High (if new attack vector could bypass Jira validation mechanism)
Configuration files	JiraSecPlugin reads from and writes to the configuration files (No asset of high value in the file such as password)	Injection (bad input,	As a defense in-depth mechanism, directory and configuration files are protected from unauthorized access. Input from config files are validated before use.	Trivial ()
JiraSecPlugin	The binary itself is an entry point to Jira Core	Binary planting (Malicious inclusion of malware)	Digital signature to validate the authenticity and integrity of the binary	Low - High