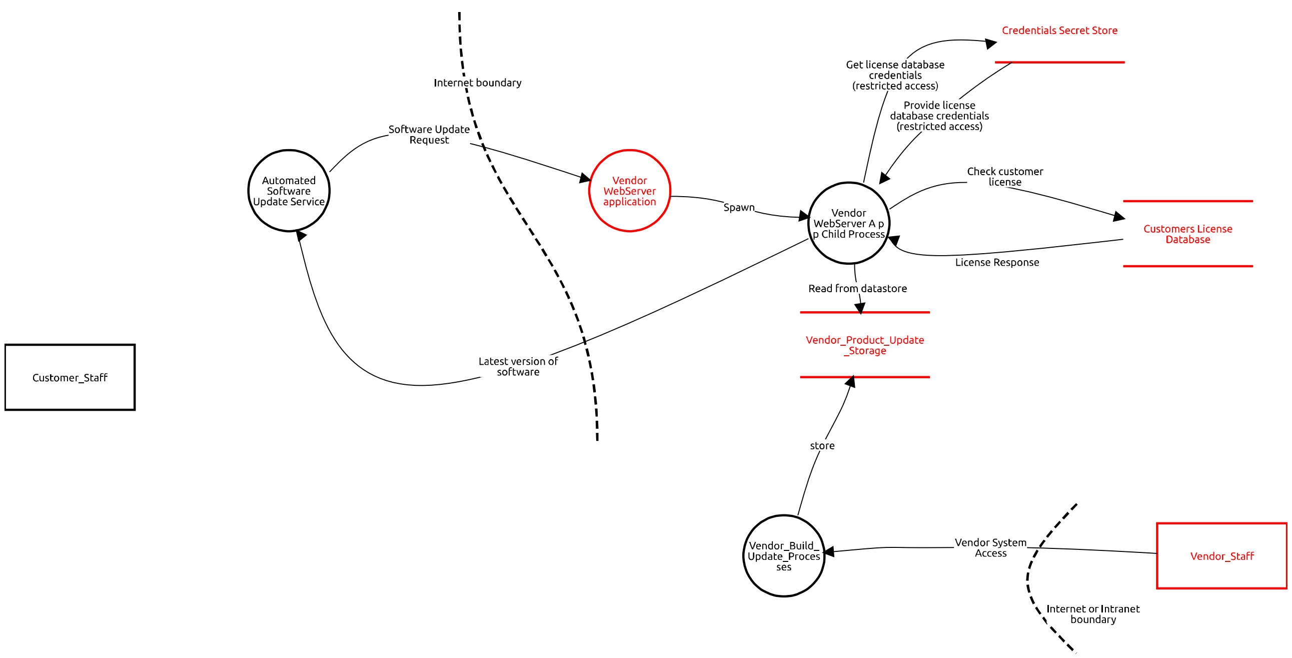
Threat model report for sample1

Owner:
Vijay
Reviewer:
Contributors:

High level system description

SoftwareUpdate


Internet boundary
Software Update Request
Automated Software Update Service
Vendor WebServer application
Spawn
Get license database credentials (restricted access)
Credentials Secret Store
Provide license database credentials (restricted access)
Check customer license
Vendor WebServer A p p Child Process
Customers License Database
License Response
Read from datastore
Vendor_Product_Update _Storage
Customer_Staff
Latest version of software
store
Vendor_Build_ Update_Proces ses
Vendor System Access
Vendor_Staff
Internet or Intranet boundary

Automated Software Update Service (Process)

Description:

The software update service provided by Vendor that updates the vendor software based on licenses.

No threats listed.

Vendor_Product_Update _Storage (Data Store)

Description:
Vendor's internet-accessible storage location, where product updates are located

Every Access to this datastore should be logged.

Repudiation, Open, Medium Severity

Description:
Malicious actors might access this datastore which might go

Mitigation:
Every access to this datastore should be logged with details such as user/role name, permissions level, ip addresses, method of access, locations/objects accessed etc.,

Customers License Database (Data Store)

Description:
Database that holds custmer licenses

Access to this database should be restricted.

Information disclosure, Open, Medium Severity

Description:
Malicious actors might access this database.

Mitigation:
This database should be in private subnets, should only have ingress open to specific processes, should have no egress & should only be accessible by specific processes with specific user/pass controls or other identity controls.

Customer license database should be encrypted both at-rest & in transit

Information disclosure, Open, Medium Severity

Description:
Malicious actors might access this database if it is not encrypted.

Mitigation:
Encrypt database

Vendor WebServer application (Process)

Description:
Vendor Web application that receives information from Software Update service & sends information about updated software

WAF protection

Tampering, Open, High Severity

Description:
Web application might be exploited.

Mitigation:
An industry standard WAF must be implemented which usually covers many attack vectors such as web attacks, sql injection attacks, anaymous ips, blacklisted ips, whitelisted ips, kernel specific exploits, buffer overflow etc

Access to Web application must be authenticated

Spoofing, Open, High Severity

Description:
Web application access must be authenticated.

Mitigation:
Web application access should be controlled by OAuth2.

Web application must be protected by a Gateway

Denial of service, Open, Medium Severity

Description:
Web application might be hit with Denial attacks, excessive rates of requests.

Mitigation:
Web application must be fronted with an API Gateway (& preferably behind load balancers in autoscaling hosts in a private subnets & not in public subnets). Rate limit thresholds should be set on API Gateway

Logging

Denial of service, Open, Medium Severity

Description:

Without logging (esp of failure attempts), repeated attempts could be made.

Mitigation:
Log all attempts (esp failed ones) & together with WAF protection, authentication controls, rate limiting should serve as mitigation against brute force tries. Also raise alarms on access failures.

Sanity check user inputted metadata that contains software versions

Tampering, Open, High Severity

Description:
Inputted metadata might contain injection data.

Mitigation:
User inputted metadata that contains software versions must be sanity checked.

Vendor WebServer App Child Process (Process)

Description:
WebApp Child process that reads the correct version of software update from datastore & sends it back to clients.

No threats listed.

Vendor_Build_ Update_Proces ses (Process)

Description:
Vendor process that builds software

No threats listed.

Vendor_Staff (External Actor)

Description:

SSO Access only

Spoofing, Open, High Severity

Description:
Local accounts should not be created for Vendor staff to access build systems, software update repository etc,

Mitigation:
ALL of these MUST be followed for mitigation. These are all combined into a single threat to keep this document small.
1. Must use SSO access associated with a corporate AD system
2. Must use MFA, hardware MFA if possible, no SMS only virtual MFA tokens
3. Must have strong password controls (ie., ALL of min password length of 17+ chars, all chars & symbols, no password reuse of last 50+ values, password rotation every 60 days). i.e., all possible strong password policy options that will force/drive the use of password manager among users

RBAC access with permissions boundaries

Elevation of privilege, Open, Medium Severity

Description:
Users who can access the system might be able to create other users/roles with higher privilege than the permission with which they logged into the system.

Mitigation:
Role Based Access Controls along with Permissions Boundaries must be setup for all users.

All user access to the systems must be logged

Repudiation, Open, High Severity

Description:
Unauthorized users can log into the system without traceability.

Mitigation:
1. All logins to the system MUST be logged.
2. for public cloud systems an entire audit trail of all actions performed in the system MUST be available.

Access to systems through VPN only for remote access

Spoofing, Open, Medium Severity

Description:
Users should not be able to access the systems from public internet if possible

Mitigation:
Setup Corporate VPN, whitelist specific IPs or IP ranges & only allow access from these.

Customer_Staff (External Actor)

Description:

No threats listed.

Vendor System Access (Data Flow)

Description:

No threats listed.

store (Data Flow)

Description:
It is assumed that the communication between the Vendor Build & Update process is on an encrypted channel over a internal/private network. If the vendor solution is implemented on public cloud, then the communication/dataflow should be preferably implemented as a privatelink that traverses on an encrypted channel over only cloud provider network as opposed to public internet over HTTPS interface.

No threats listed.

Software Update Request (Data Flow)

Description:
HTTPS request that contains metadata of installed versions.

No threats listed.

Latest version of software (Data Flow)

Description:

No threats listed.

Spawn (Data Flow)

Description:

No threats listed.

Read from datastore (Data Flow)

Description:

No threats listed.

Check customer license (Data Flow)

Description:
Check customer license against database

No threats listed.

License Response (Data Flow)

Description:

No threats listed.

Credentials Secret Store (Data Store)

Description:
DB Credentials Secret Store (better to not use DB credentials at all & instead use RBAC (eg., access DB with IAM role access with temporary credentials)

Access to this secret store should be restricted.

Information disclosure, Open, Medium Severity

Description:
Malicious actors might access this secret store to get credentials.

Mitigation:
Access to this secret store must be restricted to a narrow scope. Even read permissions to this secret store should be restricted to *specific items*. eg. if a process needs access to 2 items in the secret store, only those 2 items should be given access to & not to read entire secret store.

Get license database credentials (restricted access) (Data Flow)

Description:
Get restricted access to license database credentials

No threats listed.

Provide license database credentials (restricted access) (Data Flow)

Description:
Provide credentials for restricted access to license database

No threats listed.