advenica

Importing updates into secure production environments

To remain efficient and secure, systems must be updated regularly. For secure production environments, updates can also pose a risk of malware entering the systems. To make sure the update import is secure, special solutions are needed.

Challenge

Importing software updates securely

A great way to decrease vulnerabilies of a computer environment is to keep all software up to date. As different threats evolve, so do software vendors' efforts to counter these threats and patch any known vulnerabilities in the system. There are also examples of software update packages being used as the delivery mechanism for malware. Importing software updates to your secure production environment (if air gapped or not) should thus always be done with due diligence, taking precautions for attacks.

Solution

Update import with File Security Screener

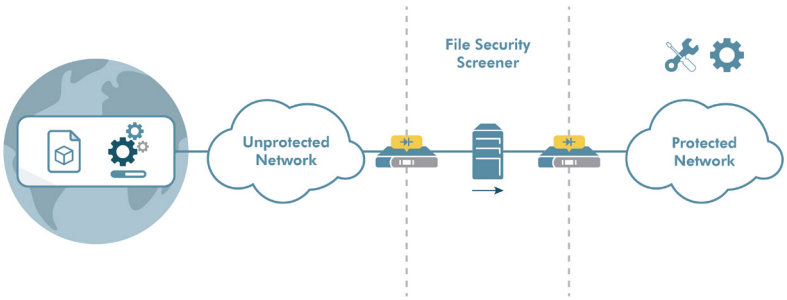
An effective way of ensuring safe SW update imports is to run the entire package through a scanning and sanitation system, such as Advenica's File Security Screener. In this case, software updates can be securely imported to the secured network, along with other files, such as virus definitions etc. Before import, all files are scanned for malware and other threats including steganography, which are actively removed using the OPSWAT MetaDefender Core and its CDR functionality. The FSS offers a vulnerability scanning to detect outdated and vulnerable dependencies in software updates that are scanned. You can mitigate known vulnerabilities even before those are installed into your production. The FSS system supports:

- Secure verified updates to your trusted production environment
- Automated workflow for bringing in update from several sources
- Reporting and analysis of the software updates and found threats
- Increased zero-day threat detection with delayed scanning procedure
- Large files, up to 100GB
- File transfer capacity: 300Mbps (scale up is possible)
- Quarantine and archive of files are supported
- Log and monitoring through Syslog and SNMP
- External heartbeat from source networks to protected network supported

© Advenica 2024

Although SW update packages can be large in size and compressed inside multiple layers, the FSS is able to open all layers for thorough scanning. The process of fetching SW updates can also be automated. The uplink data diode can be assigned to regularly scan for available updates at predefined sites and download them for scanning without manual triggering.

File Security Screener,
Importing SW updates to a secure production environment



Advantages

Preventing breaches and securing stability

There are a number of advantages when using the File Security Screener for update import.

Preventing data breaches: Ensuring updates are malware-free significantly reduces the risk of data breaches.

Maintaining system integrity: Scanning updates ensures that your system remains stable and operates as intended, preventing unauthorised alterations to system files and functionalities.

Protecting network security: By scanning updates, you prevent malware from spreading across your network, protecting multiple devices and systems from infection.

Ensuring business continuity: Ensuring updates are malware-free helps maintain uninterrupted business operations, which is crucial for maintaining productivity and service delivery.

Cost savings: Preventative scanning can save significant costs associated with addressing malware infections, including downtime, recovery efforts, and potential legal fees.

Improving user trust: Regularly updating and securing your systems increases user confidence in your software, especially if updates are provided to end users or clients.

Identifying false positives: Scanning updates helps identify legitimate software that may be incorrectly flagged as malware, allowing for timely intervention and resolution.

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more on advenica.com

© Copyright 2024 Advenica AB. All rights reserved. Advenica and the Advenica logo are trademarks of Advenica AB. All registered and unregistered trademarks included in this publication are the sole property of their respective owner. Our policy of continuous development may cause the information and specifications contained herein to change without notice. Doc. no.: 21440 v1.0

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED