

Smart Security Enhancer as a Device Guardian to Mitigate Software Vulnerabilities

Abstract

This white paper describes a new approach called Smart Security Enhancer (SSE), an in-house solution that keeps customers' devices at a safe state. It discusses how SSE proactively identifies and prioritizes security updates to reduce software vulnerabilities for customers.

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Introduction.....	4
Overview.....	4
Methodology and Solution.....	4
Data.....	4
Approaches.....	7
Architecture.....	8
Key findings.....	8
Security score for each software update.....	8
Prioritization of updates and device security score.....	9
Reaction and feedback.....	10
Key facts and take-aways.....	11
Conclusion.....	11
References.....	12
Documentation.....	12
We value your feedback.....	12



Topics:

- [Introduction](#)
- [Methodology and Solution](#)
- [Key findings](#)
- [Reaction and feedback](#)
- [Key facts and take-aways](#)
- [Conclusion](#)
- [References](#)

Introduction

Overview

As cyber attacks increase every year, cyber security has become the top priority for customers. To prevent these attacks, which usually occur due to software vulnerabilities, customers need to install the latest software updates with security patches. Currently, SupportAssist has measures to ensure that customers are aware of the latest updates for their software. As an enhancement to this solution, the ADSE team has developed Smart Security Enhancer (SSE). This program informs customers which updates are security-specific updates and how critical those security updates are.

In addition to proactively notifying customers about security updates, SSE can help manage multiple security updates. For example, if customers cannot install all available security updates at once, SSE will output a security score for any remaining security updates. This score informs customers which updates must be installed first and which can be installed in the future.

Integrating SSE with SupportAssist creates a customized model that constantly monitors your device's security score based on software vulnerabilities.

The key objectives for this solution are:

- To proactively identify security updates
- To prioritize security updates based on security severity
- To prioritize security updates and output a security score based on unfixed software vulnerabilities at device-level

Methodology and Solution

Data

This section describes each of the three datasets used for testing: Driver enumeration, Agile data, and the National Vulnerability Database (NVD).

Driver enumeration

Driver enumeration provides the latest available software updates.

The data below provides all the latest available software updates at a given time for a given device using SupportAssist. These software updates include driver, BIOS, firmware, and more.

Figure 1 displays a snippet of the available updates of a given device. **Service_tag** is a unique identifier for each device, of which have been hidden in this document for privacy purposes. **Driver_id** is also a unique identifier for each software update. For this device, there were 10 available updates.

	service_tag ▲	driver_id ▲	utc_timestamp ▲	platform ▲
1		26GC8	2020-09-17T12:32:57.423+0000	inspiron 3584
2		2V203	2020-09-17T12:32:57.423+0000	inspiron 3584
3		66CVW	2020-09-17T12:32:57.423+0000	inspiron 3584
4		CCXT7	2020-09-17T12:32:57.423+0000	inspiron 3584
5		H673V	2020-09-17T12:32:57.423+0000	inspiron 3584
6		M7G4T	2020-09-17T12:32:57.423+0000	inspiron 3584
7		R93YC	2020-09-17T12:32:57.423+0000	inspiron 3584
8		RTM33	2020-09-17T12:32:57.423+0000	inspiron 3584
9		VVRY0	2020-09-17T12:32:57.423+0000	inspiron 3584
10		YT1RF	2020-09-17T12:32:57.423+0000	inspiron 3584

Figure 1. Available updates for a Dell device

Agile data

Agile data provides fixes and enhancement information of software updates for determining security updates.

This data provides information such as name, version, vendor, release date driver id, as well as fixes and enhancements for a given update.

As shown in Figure 2, the **Fixes & Enhancements** feature displays whether a software update is a security update. In this example, the Dell Inspiron 7347 system BIOS is a security update because it contains CVE-2020-5379 under the Fixes & Enhancements section. It is also a security update because the Common Vulnerabilities and Exposures (CVE) is from Dell.

Driver ID: MK9VT

1 Dell inspiron 7347 System BIOS RESTART REQUIRED

2 This package contains the Dell system BIOS update. BIOS is a firmware that is embedded on a small memory chip on the system board. It controls the keyboard, monitor, disk drives, and other devices.

Get the latest driver

Please enter your product details to view the latest driver information for your system.

Enter Details

3 Fixes & Enhancements

- Firmware updates to address CVE-2020-5379.

Version

Version A13, A13

Category

BIOS

DELL CVE

Release date

14 Jul 2020

Importance

Urgent

Figure 2. An example of security update that contains a CVE from Dell

Driver ID: TNWDT

1 **AMD Radeon Graphics Driver** **RESTART REQUIRED**

2 This package contains the driver for AMD Radeon 610 series graphics card. A graphics or video driver is the software that enables communication between the graphics card and the operating system, games, and applications.

↓ **Get the latest driver** [Enter Details](#)
Please enter your product details to view the latest driver information for your system.

3 **Fixes & Enhancements**
- Driver update to address the AMD 2019 security update (CVE-2019-5049, CVE-2019-5098, CVE-2019-5146, CVE-2019-5147, CVE-2019-5124, CVE-2019-5183).

Version Version 26.20.15026.1, A02	Category Video
Release date 24 Jun 2020	Last Updated 24 Jun 2020
Importance Recommended	

Non-DELL CVEs

Figure 3. An example of a security update that contains third-party CVEs

Figure 3 is another example of a security update from a third-party vendor.

National Vulnerability Database

The National Vulnerability Database (NVD) is an external data source that provides information about all Common Vulnerabilities and Exposures (CVE) and their severity level.

A security update is an update that contains at least one CVE, which is a weakness in the code that hackers use to intrude computer systems. Since each CVE has a different severity level, the [National Vulnerability Database](#) should be used to determine their security severity accordingly. For this solution, the team created an internal database by mirroring the NVD. Currently, the security severity is classified into five categories:

- Low: 0.1-3.9
- Medium: 4.0-6.9
- High: 7.0-8.9
- Critical: 9.0-10.0

NOTE: Higher scores have more severe CVEs.

Figure 4 is an example of a CVE from the NVD. CVE-2020-9558 is a CVE from Adobe bridge and its base score (which determines the security severity) is 3.3.

CVE-2020-9558
Current Description
 Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.

[+View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

Base Score: 3.3 LOW Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://helpx.adobe.com/security/products/bridge/apsb20-19.html	Patch Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-125	Out-of-bounds Read	NIST

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 (hide)

Up to (including) 10.0.1

Running on/with

cpe:2.3:a:adobe:bridge:*:*:*:*:*:*

cpe:2.3:o:microsoft:windows:*:*:*:*:*:*

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figure 4. An example CVE from the NVD website

Approaches

This section describes the steps that ADSE team took to identify security updates and to prioritize them.

Step 1 - Identify the latest available updates

Driver enumeration data contains not only the latest available software updates but also all historical records of software updates. To address this issue, the ADSE team added a Window function that displays only the latest updates for each device.

Step 2 - Identify security-specific updates and corresponding severity level

Once the latest updates were identified, the following procedures were performed to identify security updates and their severity:

- Combined updates with Agile data to get “Fixes & Enhancements” information for each update.
- Applied regulation expression to extract CVEs from the “Fixes & Enhancements” feature (if any CVE exists).
- Counted the number of CVEs for each update.
- Joined with NVD data to obtain the security score and severity for each CVE.
- If a security update had more than one CVE, the ADSE team applied a “Max” function to find the CVE with the highest security score and used that score as the security score for the given update. This rule complies with the standards of the security industry. For example, a given security update could have 2 CVEs. If one update has a security score at 6.5 and the other at 8.6, the algorithm will use 8.6 as the security score for that update.
- Applied a keyword search using NVD data to identify CVEs to determine if a given CVE is from Dell.

Step 3 - Prioritize security updates and output security scores at device-level

After available updates and security updates were identified, the following steps were implemented to prioritize updates and output a security score at device level:

- Ranked the available updates based on security scores so that the display of updates is shown to customers from most critical to least critical.
- Depending on which security updates are installed and how many of them are left, the model would output the highest security score based on uninstalled security updates at the asset level. For example, a given device could have two security updates left uninstalled. If the security score of one update is 7.7 and the other is 5.5, the system algorithm will output a security score of 7.7 for that device.

Architecture

Training data is retrieved from the Agile database, while NVD and data pre-processing is applied on training data. A smart security model is created using Agile data which has "Fixes & Enhancements" information for each update and NVD that has a security score ranging from 0.0 through 10.0 for each CVE. The model assigns each update a security score that is the highest among all the possible CVEs contained within it.

As shown in Figure 5, if an update has no CVEs, the security score will be zero.

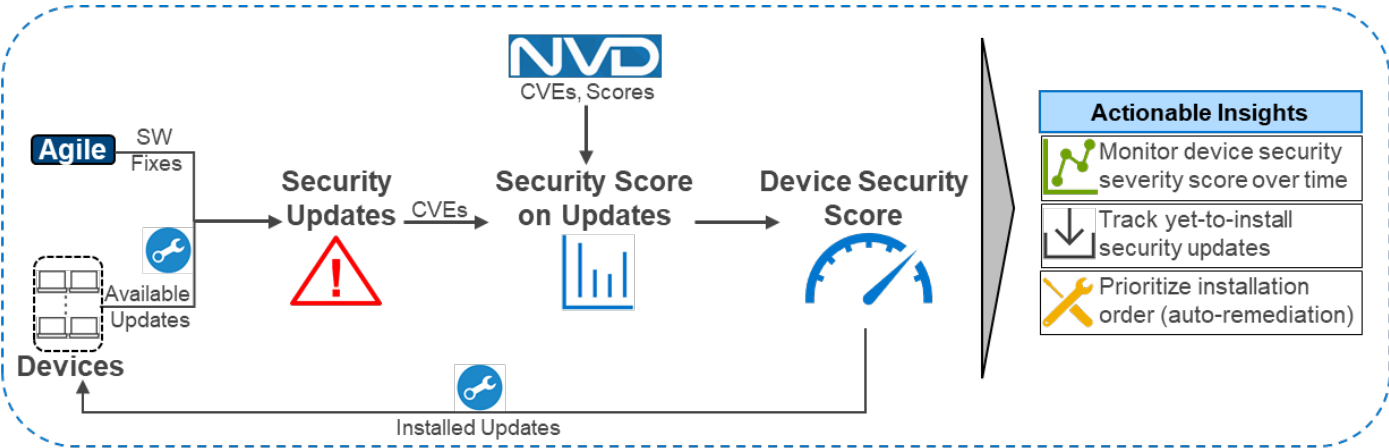


Figure 5. SSE workflow

Key findings

Security score for each software update

Regular expressions are used to identity CVEs, and "NVD" is used to describe the security severity of each CVE.

Figures 6 displays the information that is aggregated by the software.

driver_id	cve_num	security_score	security_severity
JY83M	1	9.8	CRITICAL
WR5V6	9	7.8	HIGH
7XH7G	0	0	NONE
D04NK	19	8.2	HIGH
C8NR0	1	6.7	MEDIUM
11F3M	0	0	NONE
3D5WW	0	0	NONE
660HV	0	0	NONE

Figure 6. Security score and severity at update-level

Below is a description of the headers in Figure 6:

- driver_id: a unique identifier for each software update
- cve_num: the number of CVE identified in each update
- security_score: a security score ranging from 0.0 to 10.0 (the higher the number, the more severe the security update)
- security_severity: the severity of security update (classified into none, low, medium, or high [and critical] categories)

An update with a cve_num of more than 0 is a security update. In the example above, JY83M is a security update because it has one CVE, and it is a highly critical security update because it has a security score of 9.8.

Prioritization of updates and device security score

After determining the security update and computing security score, the algorithm can prioritize software updates by ranking security scores, as shown in Figure 7.

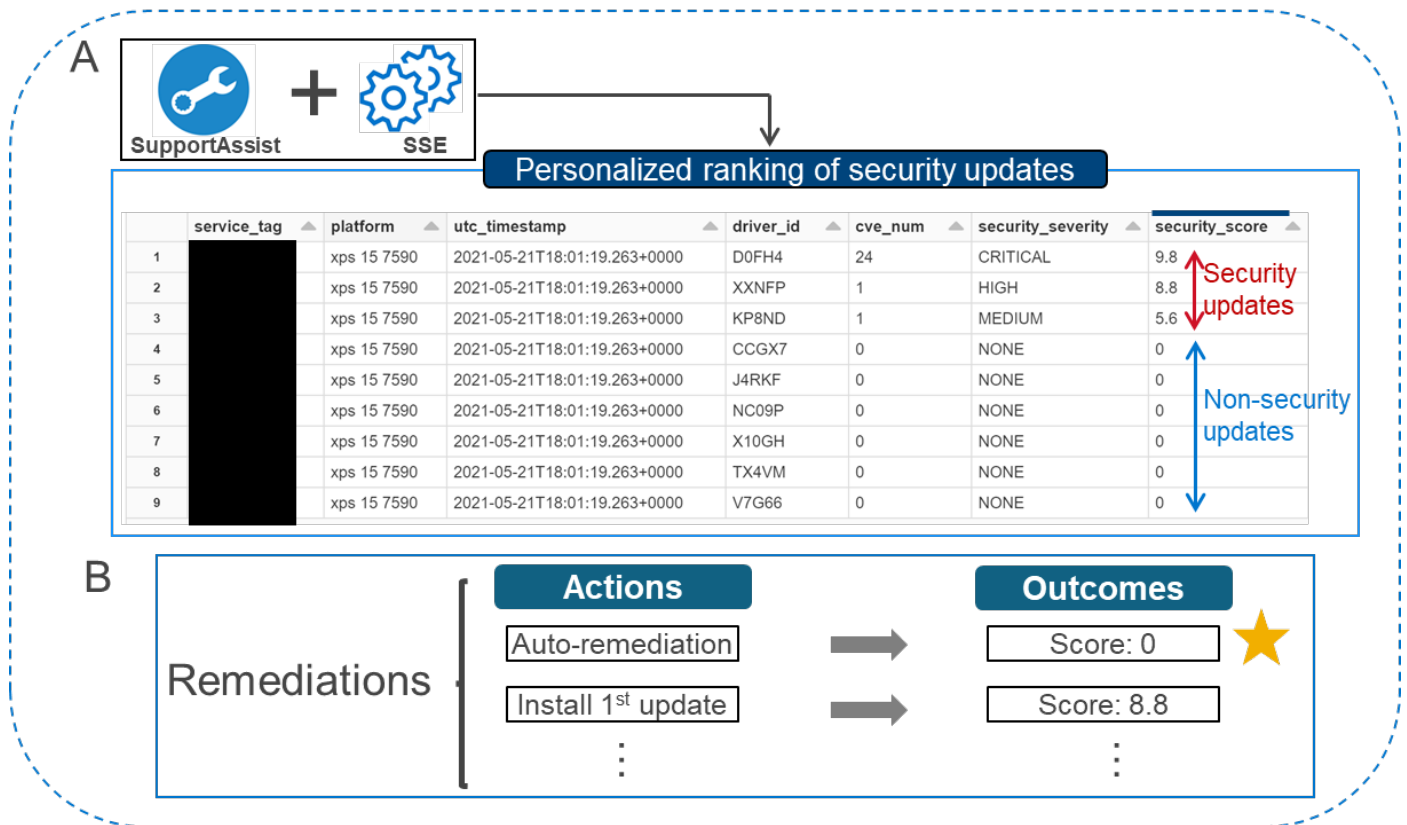


Figure 7. Prioritization of security updates and remediation

For this example, the ADSE team randomly picked an XPS 15 7590 device. Out of nine available security updates, three were security updates. A security score allows customers to see the installation order of the recommended, security-specific updates in Figure 7A.

In terms of remediation, if customers authorize vulnerable software fixes, the system can automatically install available security updates through SupportAssist. As shown in Figure 7B, when this option is implemented, the resulting device score is 0.

Reaction and feedback

Figure 8 demonstrates that the SSE identifies roughly 24 security updates and impacts nearly 74K devices on a weekly basis.

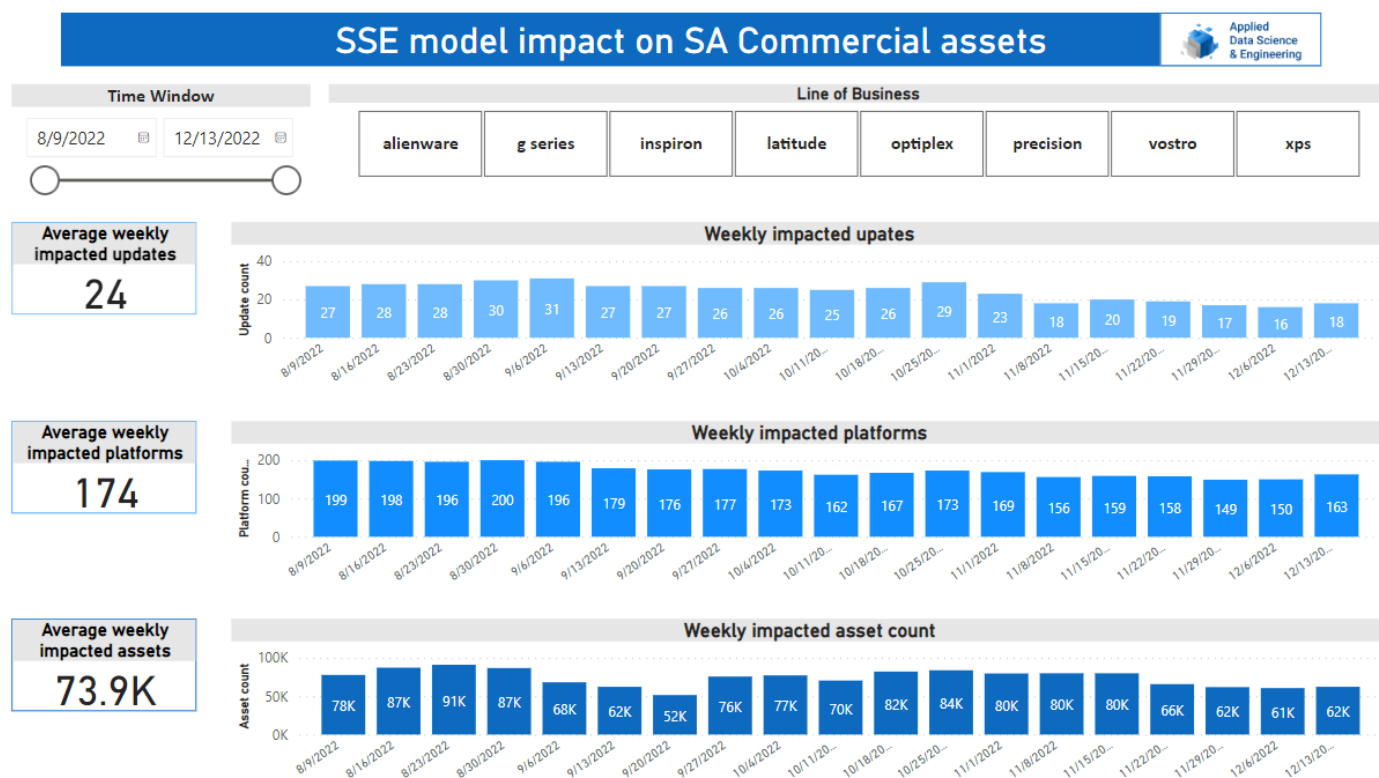


Figure 8. SSE impact monitoring

Key facts and take-aways

- **Security score at the update level:** This solution uses a systematic method to identify security updates and assign security scores at software update-level. This new update-level security score measures the criticality of each update.
- **Hyper-customized security score at device level:** As customers install different software on their devices, varied software vulnerabilities can result from each machine. SSE uniquely computes a security score based on varied vulnerabilities from different software configurations and outputs a customized score at device-level.
- **Prioritization and auto-remediation to mitigate software vulnerabilities:** This solution identifies security updates, computes scores for each, and prioritizes software updates based on the scores.
- **Applicable to both Dell and third-party software updates:** This solution not only applies to software updates from Dell but can be used on updates from third-party vendors, such as AMD, Intel Nvidia, providing more comprehensive coverage.

Conclusion

Internet of things (IoT) have become a part of daily life. Different software can be installed in IoT devices, meaning malicious attacks can intrude devices through vulnerable software. As a result, business data is more vulnerable than before. With the increasing risk of cyberattacks, cyber security should be a top priority for every company.

SSE is an intelligent algorithm that can help keep your devices at safe status. Not only does SSE proactively identify updates with security patches and labels them as security updates, it also assigns a security score for each update based on security severity. These security scores are used to prioritize the available updates and output a security score at device-level to highlight the device's vulnerable state.

References

Documentation

The following external documentation provides additional information:


- [NIST National Vulnerability Database](#)
- [A Historical and Statistical Study of the Software Vulnerability Landscape](#)
- [Study on Software Vulnerability Characteristics and Its Identification Method](#)

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team by [email](#).

Authors: WeiTa Chen, Ramya Mandava

Contributors: Niraj Shah, Vikas Sharma, Will Wilson

 **NOTE:** For links to additional documentation for this solution, see [Dell Technologies Solutions Info Hub for Artificial Intelligence](#).