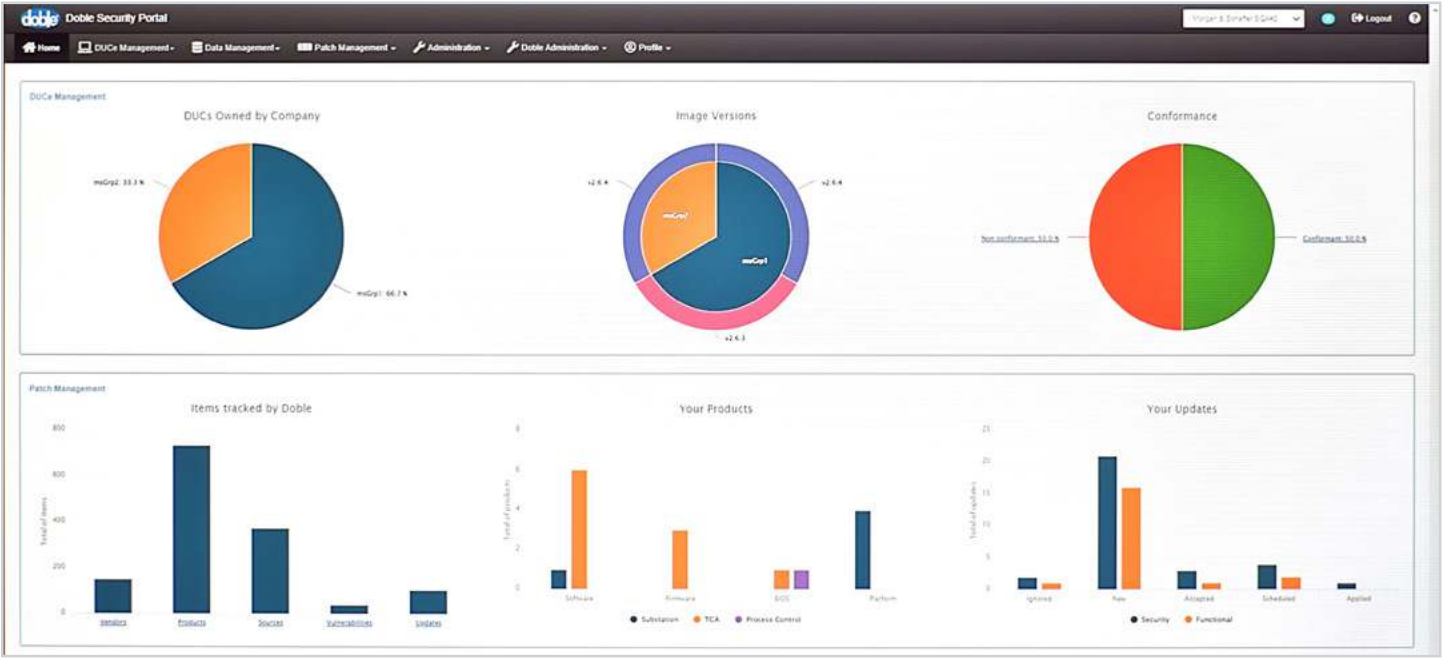
DOBLE CYBERSECURITY SOLUTIONS

PatchAssure™

Managed Security Software Patching

CENTRAL UPDATE MANAGEMENT FROM A SECURE PORTAL



Doble PatchAssure™ is a portal-based management solution that ensures IT and Compliance teams meet NERC CIP security patch and software update requirements easily, efficiently and economically. Cybersecurity experts from Doble consult with you to identify which of your cyber system products to include in your profile, then they prepare your Doble Security Portal™ access where you can login to see your CIP-reportable elements, including your transient cyber asset (TCA) fleet, and make clear-headed decisions on matters requiring your attention. Recommendations from Doble help you know when deployments are critical and which devices they affect. Workflow and compliance evidence are at your fingertips.

FEATURES

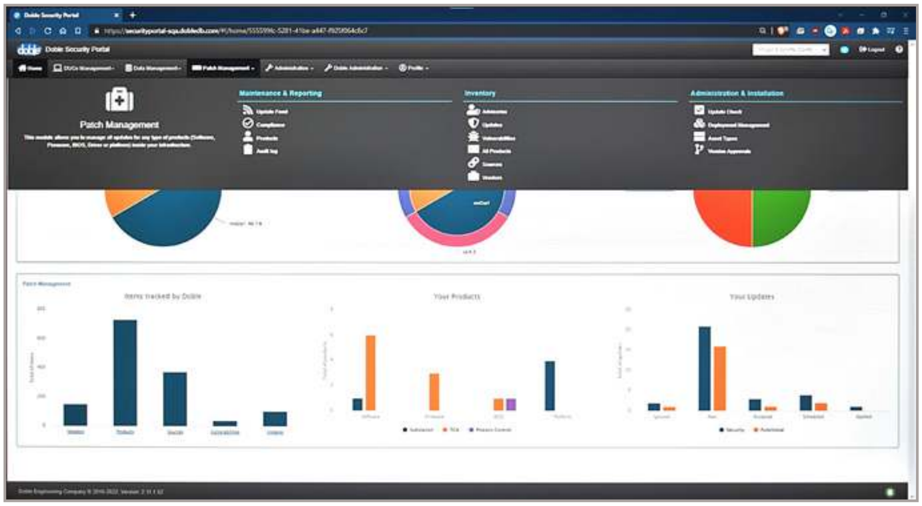
- Covers all aspects of patch management, from discovery to delivery.
- Covers all types of cyber assets, including substation devices and transient cyber asset (TCA) field computers.
- Covers all types of product updates, including security and functional enhancements.
- Modern, easy-to-use Doble Security Portal™ with comprehensive management and reporting of fleet devices and updates.

BENEFITS

- Considerable cost and resource savings compared to in-house programs.
- Quicker discovery of vulnerabilities, patches, and emerging information.
- High degree of traceability and efficiency.
- On-demand evidence for NERC CIP audits.
- Doble expertise and support every step of the way.

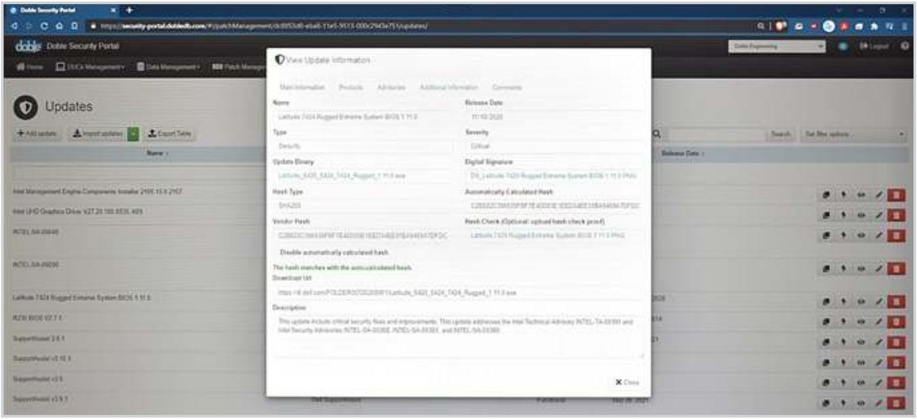
DOBLE PatchAssure™

PatchAssure is a "one-stop shop" portal-based solution for software version and security patch management. Experts from Doble monitor for the availability of updates from hundreds of sources and provide notice via the Doble Security Portal to utility administrators which includes analytics and recommendations. The multi-factor authentication the Doble Security Portal provides prevents unauthorized access to clients' CIP asset information.



MONITORING

- All asset inventory is checked for patches on a weekly basis
- Software functional update availability for applications
- Advisories concerning patches and updates



View Update Information

Main Information | Products | Advisories | Additional Information | Comments

Name: Latitude 7424 Rugged Extreme System BIOS 1.11.0

Release Date: 11/10/2020

Type: Security

Severity: Critical

Update Binary: Latitude_5420_5424_7424_Rugged_1.11.0.exe

Digital Signature: DS_Latitude 7424 Rugged Extreme System BIOS 1.11.0.PNG

Hash Type: SHA256

Automatically Calculated Hash: [illegible]

Vendor Hash: [illegible]

Hash Check (Optional: upload hash check proof): Latitude 7424 Rugged Extreme System BIOS 1.11.0.PNG

Disable automatically calculated hash

The hash matches with the auto calculated hash.

Download Url: https://dl.dell.com/FOLDER[illegible]/Latitude_5420_5424_7424_Rugged_1.11.0.exe

Description: This update include critical security fixes and improvements. This update addresses the Intel Technical Advisory INTEL-TA-00391 and Intel Security Advisories INTEL-SA-00358, INTEL-SA-00381, and INTEL-SA-00389.

QUESTIONS TO ASK

- Does the patch address a security vulnerability or weakness?
- Does the patch offer a new security feature or improved software performance?

ANALYSIS

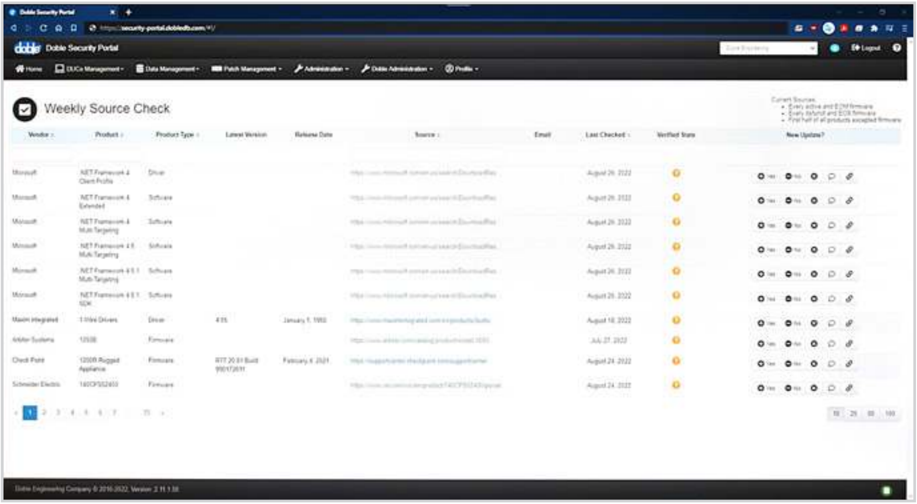
- Purpose and criticality of patches and updates
- Cyber security vulnerabilities addressed by patches and updates
- Validation of patch and update sources - URLs, RSS feeds, email lists, etc.

VISIBILITY

- Individual decisions on patching/updating and timelines
- Lifecycle of patches and updates - New, Accepted, Scheduled, etc.
- History of patches and updates by product

TRACKING

- On-demand access to patch, update, and TCA details
- Workflow actions regarding patches, updates and TCAs
- Management of users and notifications



Weekly Source Check

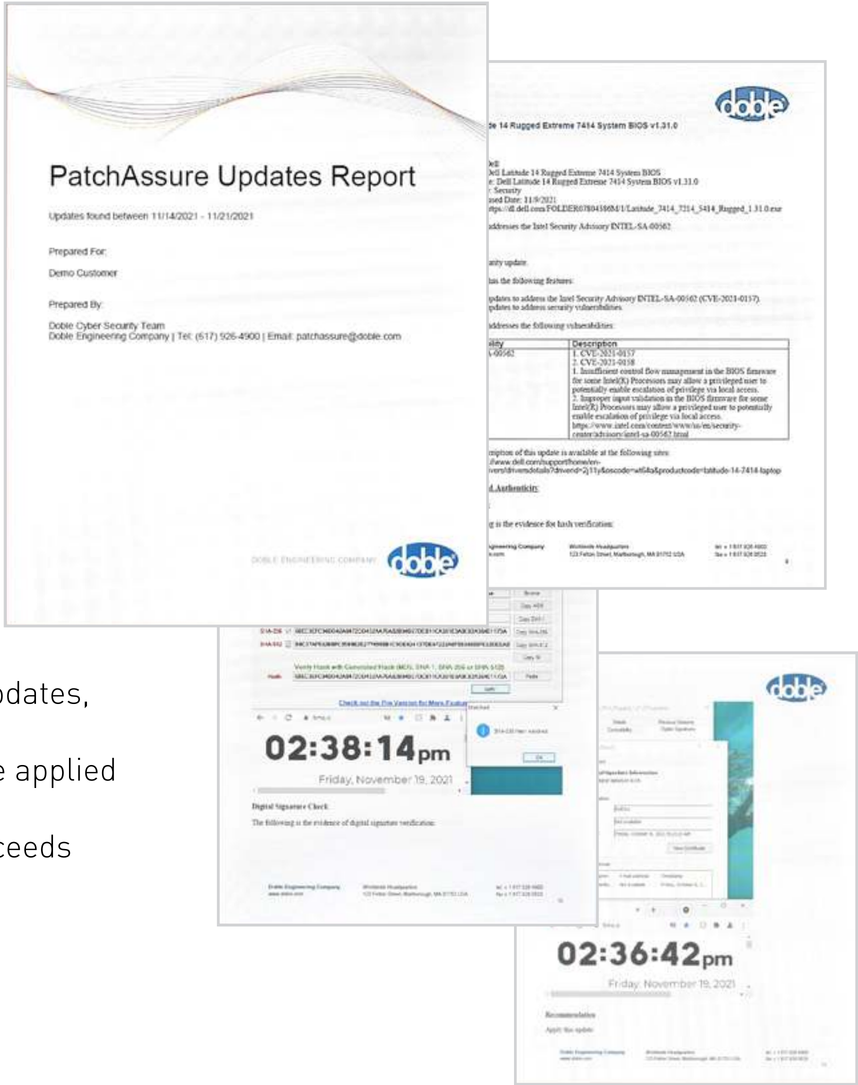
Current Sources:
- Every active and EOM firmware
- Every default and EOS firmware
- First half of all products excepted firmware

Vendor	Product	Product Type	Latest Version	Release Date	Source	Email	Last Checked	Verified State	New Update?
Microsoft	.NET Framework 4 Client Profile	Driver			[illegible]		August 26, 2022	●	⊕ Yes ⊖ No
Microsoft	.NET Framework 4 Extended	Software			[illegible]		August 26, 2022	●	⊕ Yes ⊖ No
Microsoft	.NET Framework 4 Multi Targeting	Software			[illegible]		August 26, 2022	●	⊕ Yes ⊖ No
Microsoft	.NET Framework 4.5 Multi Targeting	Software			[illegible]		August 26, 2022	●	⊕ Yes ⊖ No
Microsoft	.NET Framework 4.5.1 Multi Targeting	Software			[illegible]		August 26, 2022	●	⊕ Yes ⊖ No
Microsoft	.NET Framework 4.5.1 SDK	Software			[illegible]		August 26, 2022	●	⊕ Yes ⊖ No
Maxim Integrated	1-Wire Drivers	Driver	4.15	January 1, 1980	[illegible]		August 18, 2022	●	⊕ Yes ⊖ No
Arbiter Systems	1250B	Firmware			[illegible]		July 27, 2022	●	⊕ Yes ⊖ No
Check Point	1200R Rugged Appliance	Firmware	R77.20.81 Build 990172611	February 4, 2021	[illegible]		August 24, 2022	●	⊕ Yes ⊖ No
Schneider Electric	140CPS52400	Firmware			[illegible]		August 24, 2022	●	⊕ Yes ⊖ No

‹ 1 2 3 4 5 6 7 … 15 ›

10 25 50 100

Doble Engineering Company © 2016-2022, Version 2.11.1.38



PatchAssure Updates Report

Updates found between 11/14/2021 - 11/21/2021

Prepared For:

Demo Customer

Prepared By:

Doble Cyber Security Team
Doble Engineering Company | Tel: (617) 926-4900 | Email: patchassure@doble.com

DOBLE ENGINEERING COMPANY

de 14 Rugged Extreme 7414 System BIOS v1.31.0

Dell
Dell Latitude 14 Rugged Extreme 7414 System BIOS
e: Dell Latitude 14 Rugged Extreme 7414 System BIOS v1.31.0
: Security
ased Date: 11/9/2021
ttps://dl.dell.com/FOLDER07804398M/1/Latitude_7414_7214_5414_Rugged_1.31.0.exe

ddresses the Intel Security Advisory INTEL-SA-00562

rity update

has the following features:

pdates to address the Intel Security Advisory INTEL-SA-00562 (CVE-2021-0157).
pdates to address security vulnerabilities.

ddresses the following vulnerabilities:

ility	Description
A-00562	1. CVE-2021-0157 2. CVE-2021-0158 1. Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. 2. Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html

ription of this update is available at the following sites:
//www.dell.com/support/home/en-
vers/driversdetails?driverid=2j11y&oscode=wt64a&productcode=latitude-14-7414-laptop

d Authenticity:

g is the evidence for hash verification:

02:38:14pm

Friday, November 19, 2021

Digital Signature Check

The following is the evidence of digital signature verification:

02:36:42pm

Friday, November 19, 2021

Recommendation

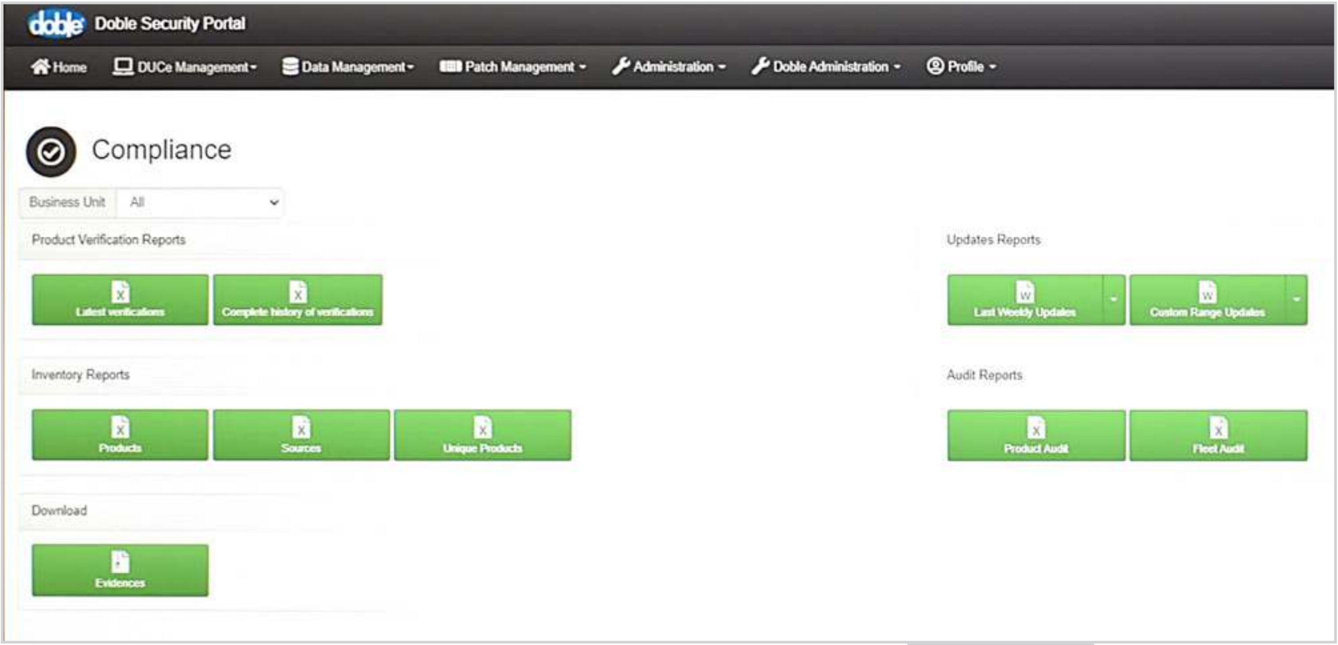
Apply the update

REPORTING

- Weekly report of relevant patches/updates, vulnerabilities, and advisories
- Proof that patches and updates were applied and sources were checked
- Auditable evidence that meets or exceeds NERC CIP requirements

NERC CIP COMPLIANCE READINESS

Leverage the tracking and reporting tools that PatchAssure provides to improve your company's NERC CIP-7 and NERC CIP-10 compliance stance:



CIP-007-6 R2 - Security Patch Management *Patch sources being tracked must be documented; at least once every 35 days, patches must be evaluated for applicability; within 35 following evaluation, patches must either be applied, or create a dated mitigation plan, or revise an existing mitigation plan.*	1. Patch sources are documented and also monitored for availability of patches. 2. Patches retrieved are analyzed for applicability and recommendations are given per classification criteria being met. Patch sources are checked weekly.
CIP-010-3 R1 1.6 - Configuration Change Management and Vulnerability Assessments *Software being patched must be verified for integrity and the source must be identified.*	1. *Patch integrity verifications are performed.* 2. *Patch sources are identified.* 3. *Details are provided in weekly reports.*

Doble Engineering Company
Worldwide Headquarters
123 Felton Street, Marlborough, MA 01752 USA
tel +1 617 926 4900 | fax +1 617 926 0528
www.doble.com

Specifications are subject to change without notice.
Doble is an ISO 9001 & ISO/IEC 17025 & 17034 Certified Company.
Doble is an ESCO Technologies Company.
PUBLISHED: OCTOBER, 2022