Critical SAP RECON Vulnerability:
Who Is At Risk & How to Protect Your Business

Frederik Weidemann, Onapsis

onapsis

Welcome and Introductions

Frederik Weidemann, Onapsis

As Chief Technical Evangelist, Frederik is driving innovation that keeps Onapsis on the cutting edge of the Business-Critical Application Security market, addressing some of the most complex problems that organizations are currently facing while managing and securing their ERP landscapes. He focused on ERP and SAP Security for the last fourteen years and is the co-author of the first book on Secure ABAP Programming.

ONAPSIS | THE WORLD'S LEADING THREAT RESEARCH ON MISSION-CRITICAL APPLICATION SECURITY

Discovered
800+
zero-day vulnerabilities in business-critical apps

Knowledgebase of
10,000+
vulnerabilities and attacks on business applications

Mitigated
60%
of SAP HANA unpatched vulnerabilities

300+
Customers

4
US DHS critical alerts based on our research

17
Patents, 8 issued & 9 pending

Discovered
33%
critical SAP vulnerabilities in the last 5 years

Featured In

REUTERS · WALL STREET JOURNAL · CNBC · Forbes · FORTUNE

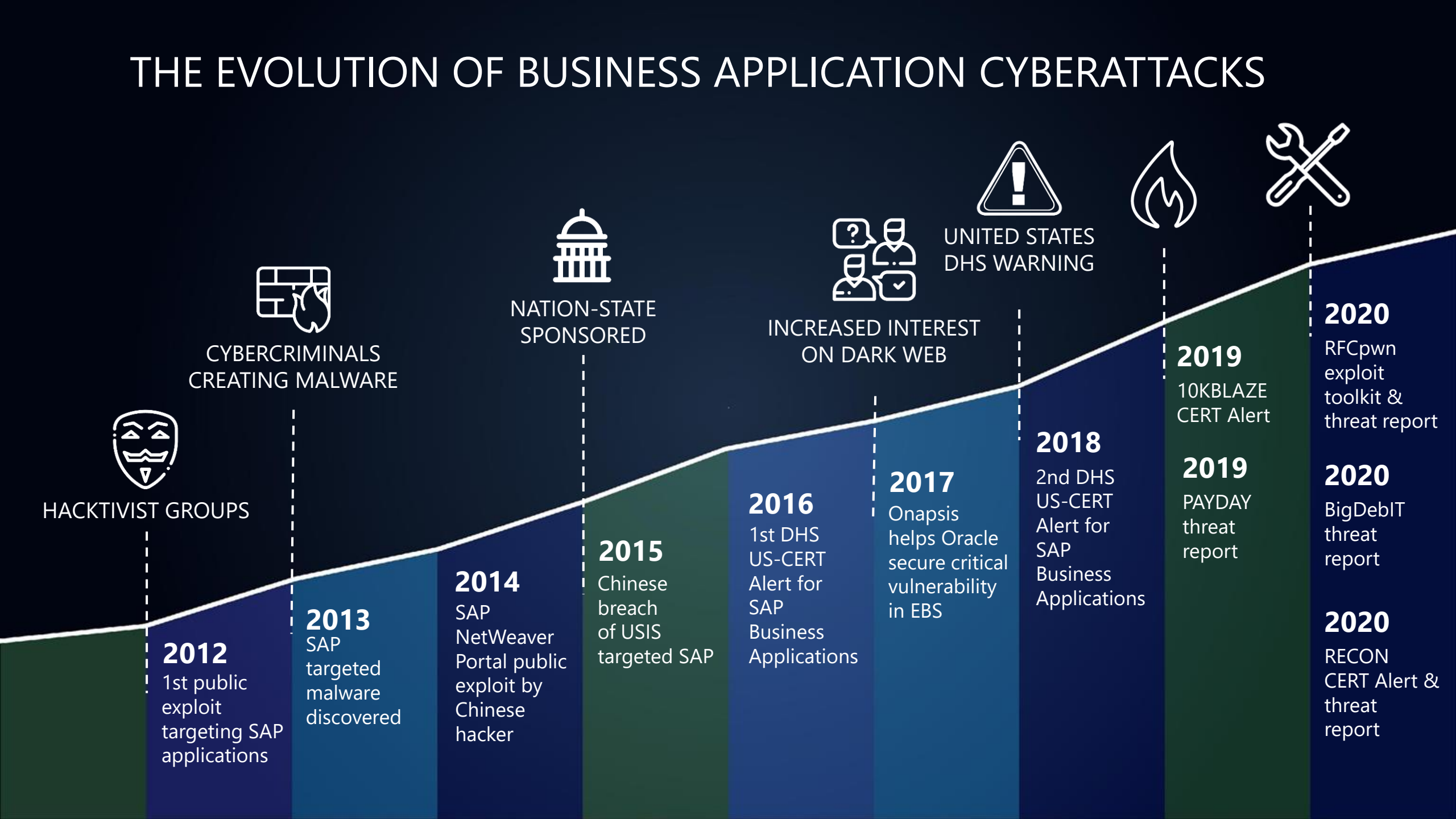
onapsis

BUSINESS APPLICATIONS DRIVE MISSION-CRITICAL OPERATIONS

"If SAP goes down, it would cost my organization $22M per minute."

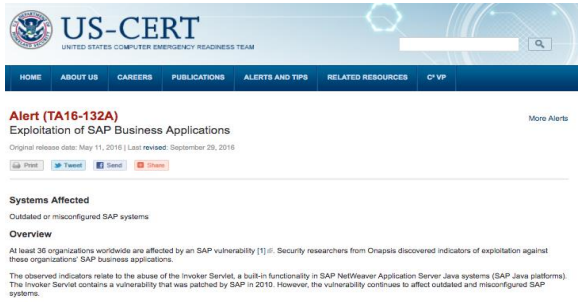
—CISO, Fortune 500 organization

THE EVOLUTION OF BUSINESS APPLICATION CYBERATTACKS



History of US CERT Alerts

May 2016



Onapsis Research Labs discovers 36 organizations worldwide being exploited through an SAP-specific vulnerability

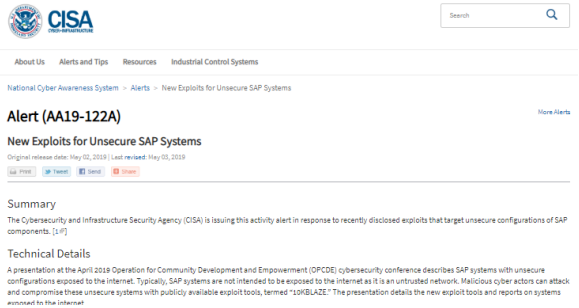
US-CERT released activity alert TA16-132A

July 2018

DHS releases second current activity alert for ERP systems

Based on report from Digital Shadows and Onapsis describing increase in threat activity and exploitation of vulnerabilities in ERP applications

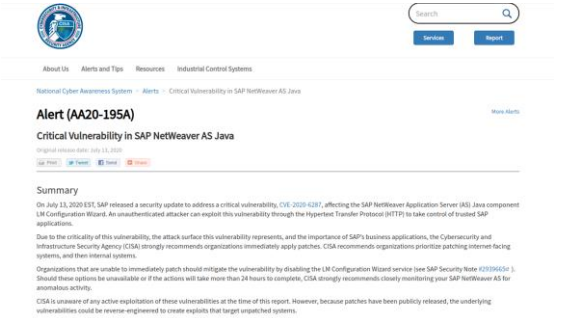
May 2019



DHS releases Critical Alert in response to publicly disclosed exploits target misconfigurations of SAP Applications (10KBLAZE)

US-CERT released activity alert AA19-122A

July 2020



US-CERT in coordination with international CERTs, release a critical alert in response to critical CVSS 10 vulnerability affecting potentially Internet-Facing SAP Applications

US-CERT released activity alert AA20-195A

onapsis

What is the SAP RECON vulnerability?

- Critical vulnerability affecting a default component present in every SAP application running the SAP NetWeaver Java technology stack 7.30 and above.
- CVE-2020-6287
- CVSS score = 10 out of 10
- A successful exploit could impact confidentiality, integrity and availability of mission-critical SAP applications.
- https://www.onapsis.com/recon-sap-cyber-security-vulnerability
- SAP Security Note 2934135 and FAQ OSS Note 2948106

onapsis

Is my organization at risk?

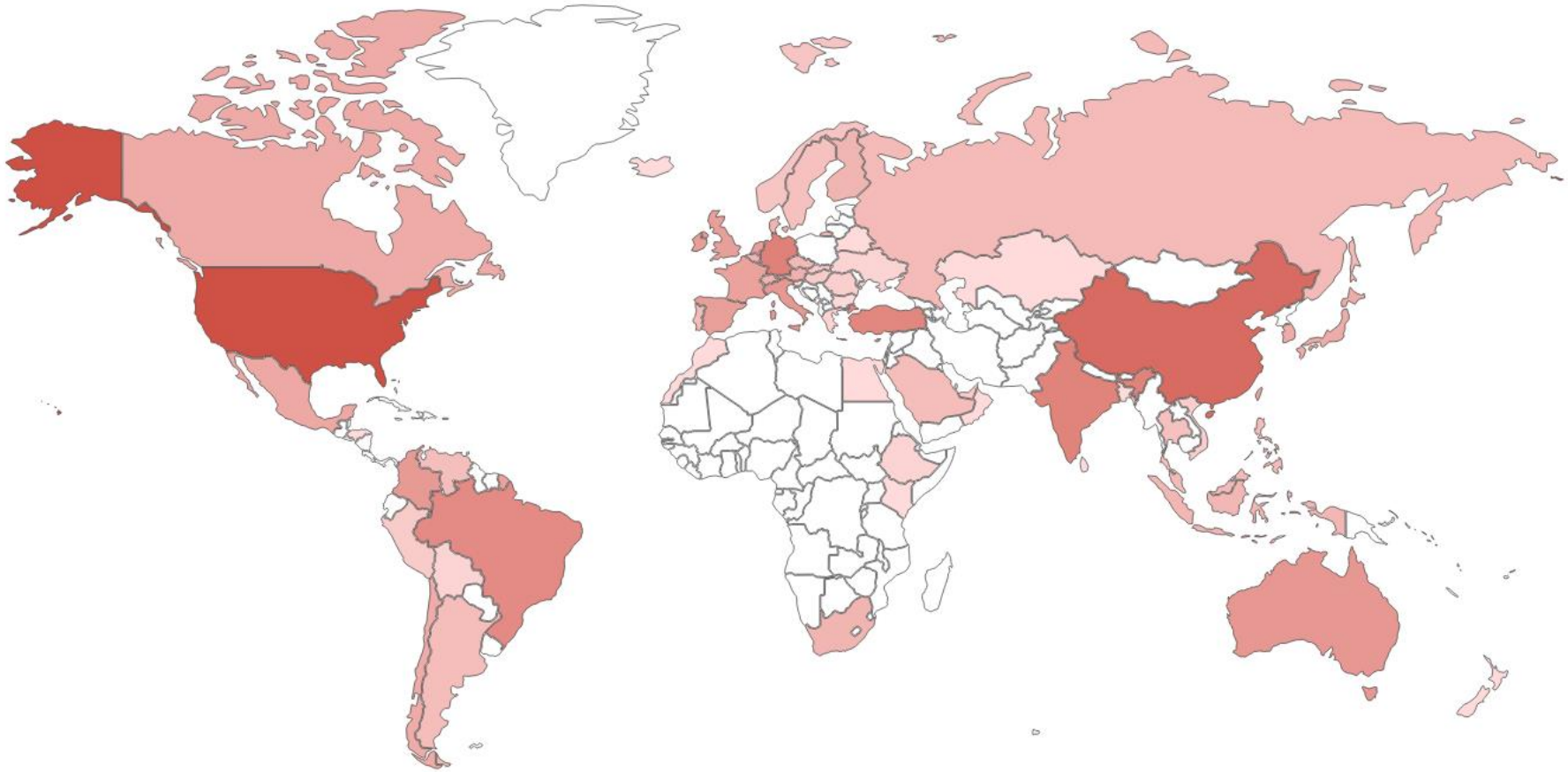
- Over 40,000 SAP enterprise customers may have been affected
  - All unpatched Java systems running on SAP NetWeaver AS Java 7.30+ are affected
  - Almost every business suite and S/4HANA customer affected due to interconnectivity with SolMan, PI, SAP Enterprise Portal
- At least 2,500 confirmed vulnerable SAP systems exposed to the internet (July 2020)
  - 33% in North America
  - 29% in Europe
  - 27% in Asia-Pacific
- Affects internal systems as well

AS Java is or may be used in:

- **SAP Enterprise Resource Planning**
- **SAP Product Lifecycle Management**
- **SAP Customer Relationship Management**
- **SAP Supply Chain Management**
- **SAP Supplier Relationship Management**
- **SAP NetWeaver Business Warehouse**
- **SAP Business Intelligence**
- **SAP NetWeaver Mobile Infrastructure**
- **SAP Enterprise Portal**
- **SAP Process Orchestration/Process Integration**
- **SAP Solution Manager**
- **SAP NetWeaver Development Infrastructure**
- **SAP Central Process Scheduling**
- **SAP NetWeaver Composition Environment**
- **SAP Landscape Manager**

onapsis

Internet exposure



Continent	Total	Percentage
Africa	20	0.80%
Asia	605	24.09%
Europe	598	23.82%
Middle East	146	5.81%
North America	836	33.29%
Oceania	69	2.75%
South America	231	9.20%
Not Specified	6	0.24%
Total	2511	100.00%

onapsis

SAP RECON VULNERABILITY

OBSERVED THREAT ACTIVITY

PATCHES & ALERTS

7/13/2020

SAP issues patches for RECON. U.S. DHS/CISA issues alert

GLOBAL ALERTS

7/14/2020

Additional cybersecurity agencies across the globe issue notes and alerts

1ST VULNERABILITY POC

7/15/2020

A vulnerability proof-of-concept is published to GitHub that can exploit Path Traversal and detect vulnerable systems

MASS SCANNING STARTS

7/16/2020

Mass scanning activity detected for systems vulnerable to CVE-2020-6287

PUBLIC FUNCTIONAL EXPLOIT

7/17/2020

Functional code targeting RECON to create an unauthorized SAP user, seen on GitHub

EXPLOIT CODE FOR SALE

7/19/2020

Exploit code to create an unauthorized SAP admin user, dump database and execute commands posted for sale for 5 Bitcoin (est. $48K USD)

SUCCESSFUL EXPLOIT CODE CONFIRMED

7/22/2020

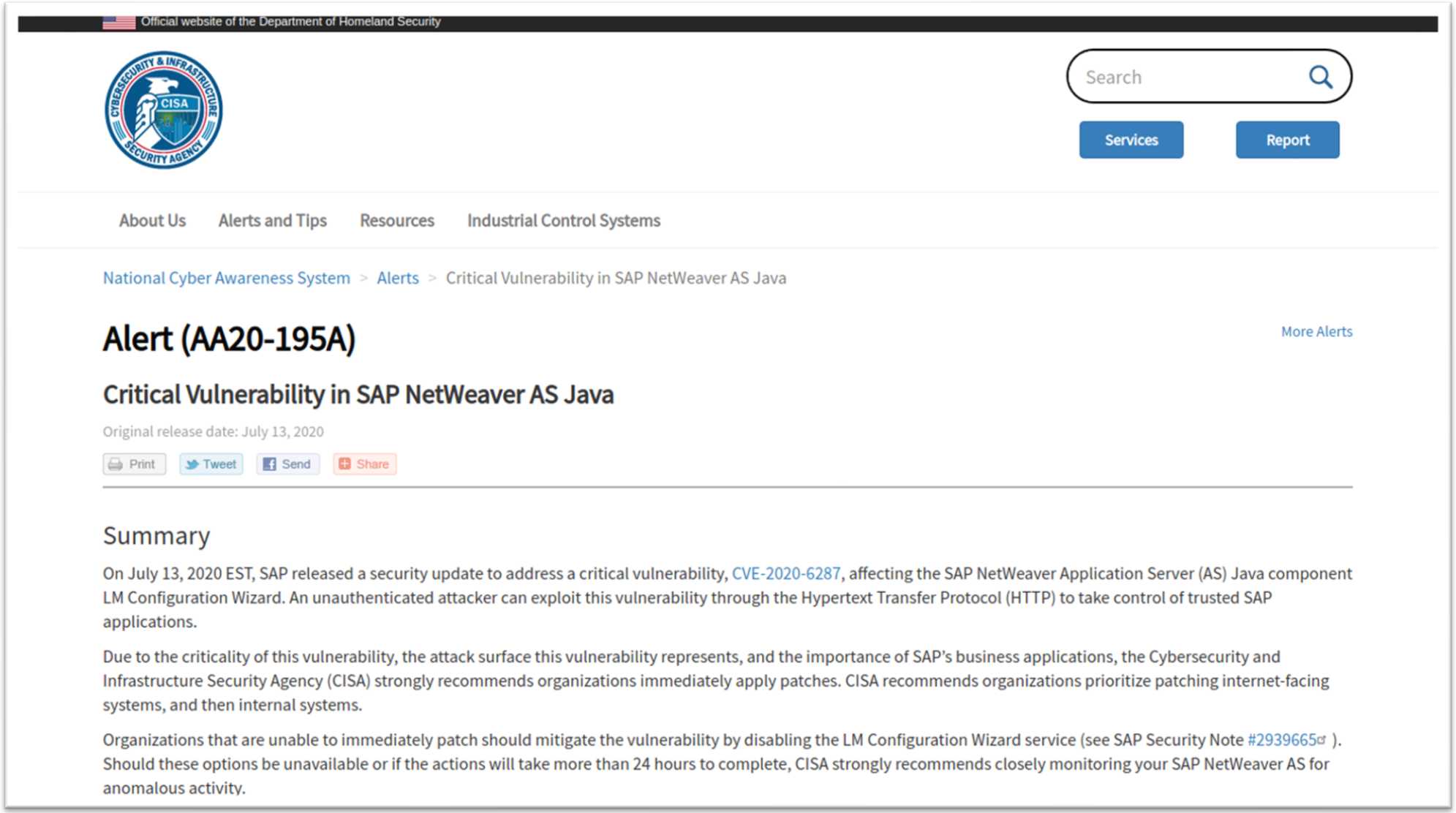
Onapsis Research Labs confirms successful exploit code to create an unauthorized SAP admin user is available

onapsis

Why is this vulnerability so critical?

- CVSS 10
- Unauthenticated
- Full impact on confidentiality, availability and integrity
- Exploitable through HTTP!
- Present in a component that is typically internet-facing and enabled by default: LM Configuration Wizard
- Present in a technology that serves typically as middleware to connect to other applications
- Affects a technology that supports critical business processes

Why is this vulnerability so critical?



Official website of the Department of Homeland Security

Search

Services | Report

About Us | Alerts and Tips | Resources | Industrial Control Systems

National Cyber Awareness System > Alerts > Critical Vulnerability in SAP NetWeaver AS Java

Alert (AA20-195A)

More Alerts

Critical Vulnerability in SAP NetWeaver AS Java

Original release date: July 13, 2020

Print | Tweet | Send | Share

Summary

On July 13, 2020 EST, SAP released a security update to address a critical vulnerability, CVE-2020-6287, affecting the SAP NetWeaver Application Server (AS) Java component LM Configuration Wizard. An unauthenticated attacker can exploit this vulnerability through the Hypertext Transfer Protocol (HTTP) to take control of trusted SAP applications.

Due to the criticality of this vulnerability, the attack surface this vulnerability represents, and the importance of SAP's business applications, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends organizations immediately apply patches. CISA recommends organizations prioritize patching internet-facing systems, and then internal systems.

Organizations that are unable to immediately patch should mitigate the vulnerability by disabling the LM Configuration Wizard service (see SAP Security Note #2939665). Should these options be unavailable or if the actions will take more than 24 hours to complete, CISA strongly recommends closely monitoring your SAP NetWeaver AS for anomalous activity.

onapsis

CVE-2020-6287 exploitation demonstration

1. Normal usage of an SAP Java System
2. Exploitation of unauthenticated service
3. Lateral movement
4. Compromise of business information
   - PII Information
   - Financial data
5. Business disruption: System shutdown

How do I protect my organization?

Apply the SAP Security Note 2934135 IMMEDIATELY

(An FAQ is provided in OSS Note 2948106)

Download the Onapsis Threat Report

- Discusses vulnerability details and business impact
- Recommendations to secure your SAP systems

Request a Cyber Risk Assessment

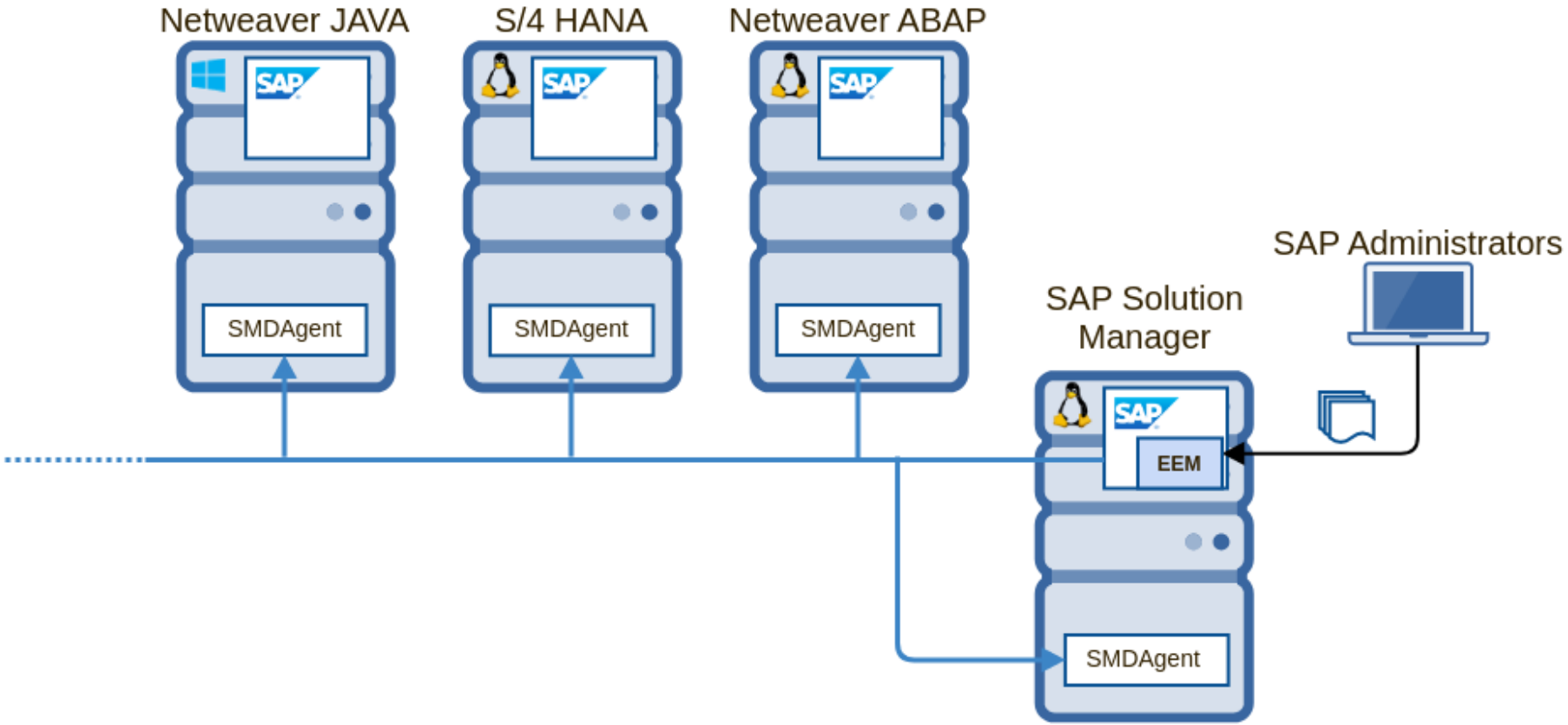
- Identify if the RECON vulnerability (and others) is present in your SAP systems
- Understand the business impact

Black Hat USA 2020 exploitation demonstration

1. Exploitation of EEM
2. Exploitation of SMDagent
3. Lateral movement with SAP Control escalating to root privileges on SAP landscape

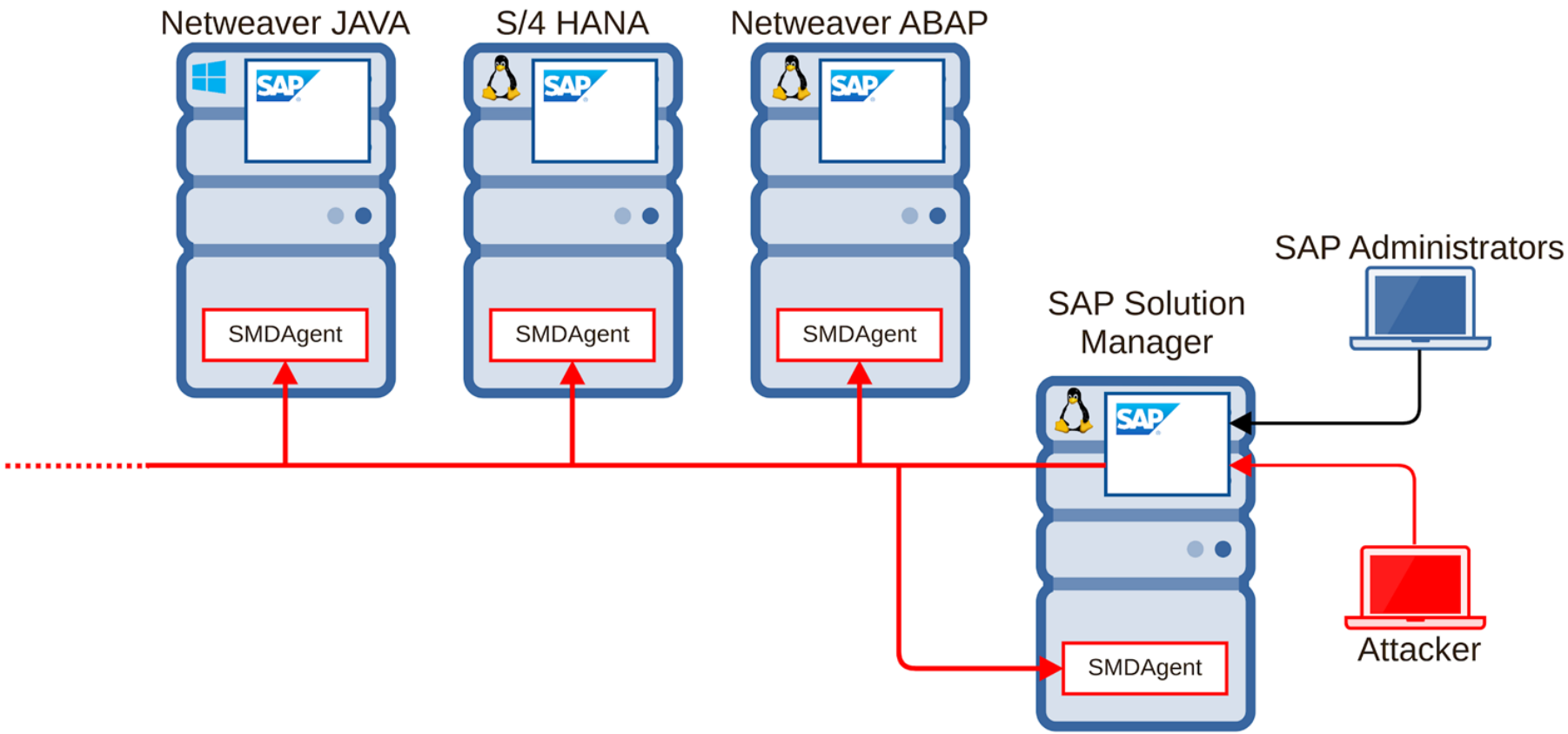
Risk: Failure to understand SAP patch management

Example Blackhat USA 2020: P. Artuso & Y. Genuer (Onapsis)



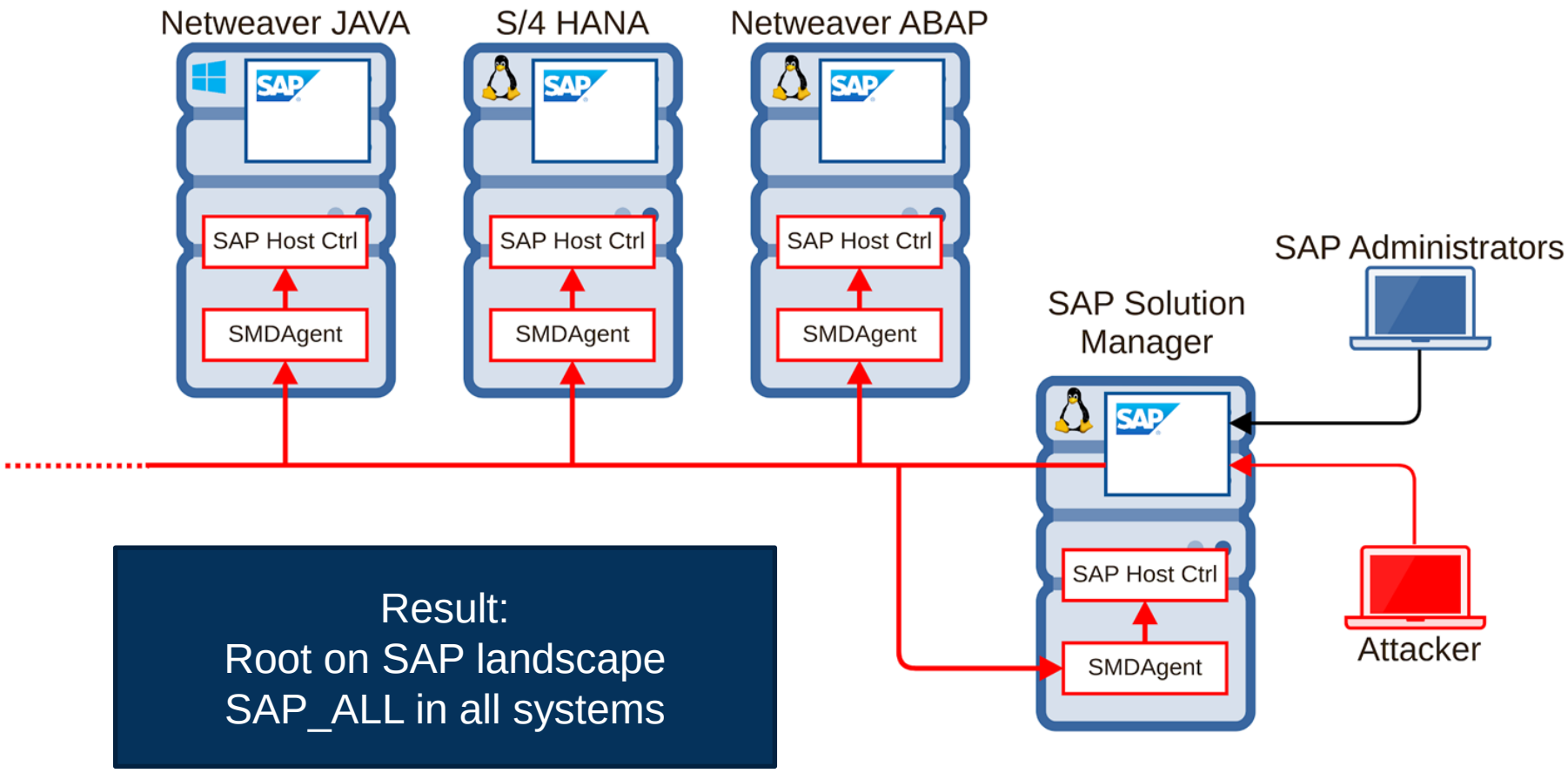
Risk: Failure to understand SAP patch management

Example Blackhat USA 2020: P. Artuso & Y. Genuer (Onapsis)



Risk: Failure to understand SAP patch management

Example Blackhat USA 2020: P. Artuso & Y. Genuer (Onapsis)



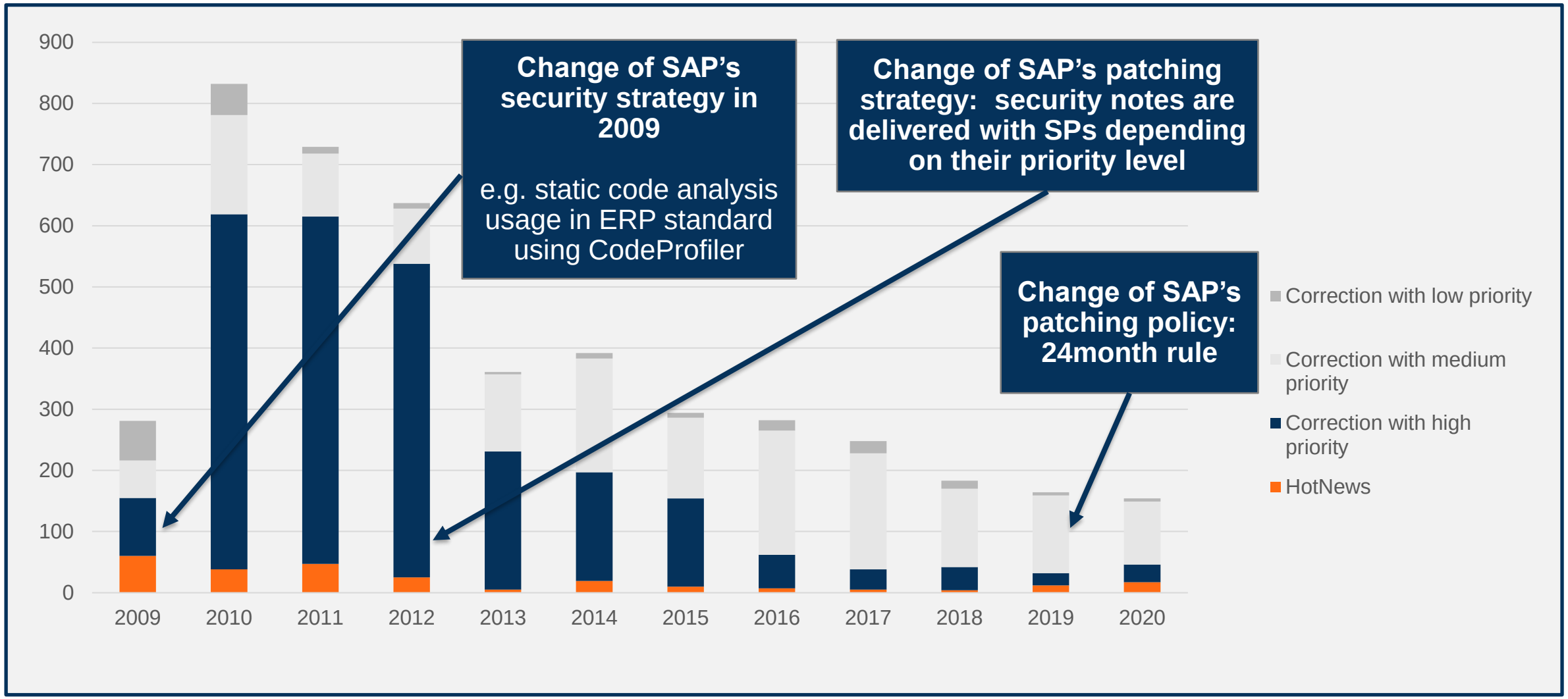
Result:
Root on SAP landscape
SAP_ALL in all systems

Black Hat USA 2020: “An Unauthenticated Journey to Root”

Related SAP OSS Notes from Onapsis Research Labs

- Patch 2902645 https://launchpad.support.sap.com/#/notes/2902645
- Patch 2902456 https://launchpad.support.sap.com/#/notes/2902456
- Patch 2890213 https://launchpad.support.sap.com/#/notes/2890213
- Patch 2808158 https://launchpad.support.sap.com/#/notes/2808158
- Patch 2823733 https://launchpad.support.sap.com/#/notes/2823733
- Patch 2839864 https://launchpad.support.sap.com/#/notes/2839864
- Patch 2849096 https://launchpad.support.sap.com/#/notes/2849096
- Patch 2772266 https://launchpad.support.sap.com/#/notes/2772266
- Patch 2738791 https://launchpad.support.sap.com/#/notes/2738791
- Patch 2748699 https://launchpad.support.sap.com/#/notes/2748699
- Patch 2845377 https://launchpad.support.sap.com/#/notes/2845377
- Patch 2904933 https://launchpad.support.sap.com/#/notes/2904933

Overview of released SAP® security notes (25.09.2020)



onapsis

What is the impact to my organization?

- Unauthenticated attacks – No user credentials
  - Internal/external
  - Bypass existing SoD and access controls
  - Potentially leaves no trace of activity
- Malicious activities
  - Modify financial records
  - View personal identifiable information (PII)
  - Corrupt data
  - Delete or modify logs and traces and other actions that put essential business operations at risk.
- Deficiency in IT controls for regulatory mandates
  - *“This vulnerability can lead to compromise of vulnerable SAP installations, including the modification or extraction of highly sensitive information, as well as the disruption of critical business processes”*

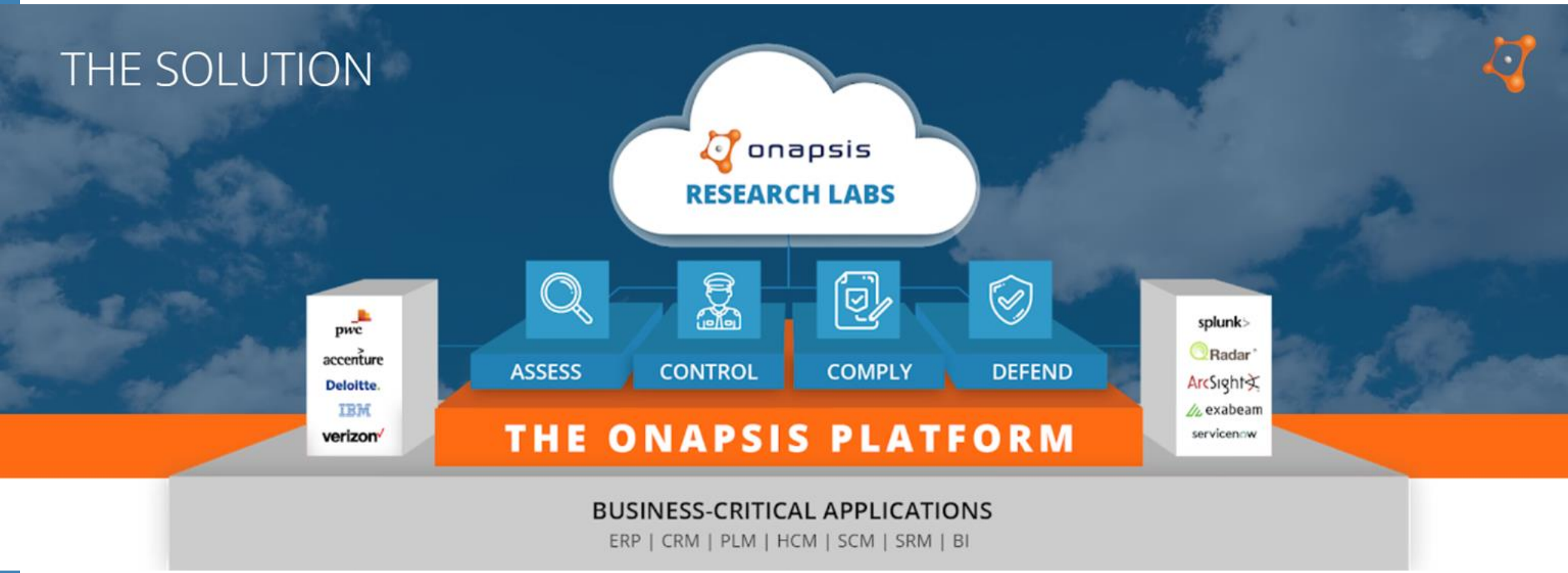
What is the impact to my organization?

What can be done and how does it affect compliance regulations?

- Extraction of personal identifiable information (PII) from customers, employees, vendors and partners
- Create fake vendors/employees and pay them
- Create & modify purchase orders & invoices
- Change bank accounts for existing records
- Release shipments
- Change inventory data
- Generate corrupted management reports
- Delete all traces of malicious action

onapsis

THE SOLUTION



The Onapsis Platform

Assess

System, interface, and deployed code assessment

Identify misconfigurations and vulnerabilities and measure business impact

Streamline prioritization and tracking of fixes for code and system issues

Control

Manage and control change to ensure system stability and integrity

Lock/block changes to prevent security and compliance issues

Automated remediation of code errors and vulnerabilities

Comply

Automate the continuous process of testing and validating compliance controls

Define, manage and run compliance policies

Receive alerts on compliance failures and understand the impact

Defend

Continuous monitoring for cyberattacks, privilege misuse and material weakness

Investigate, respond and mitigate incidents

Automate alarm notifications and SIEM integration

onapsis

More Information

- Black Hat USA 2020 “An Unauthenticated Journey to Root“
  - https://i.blackhat.com/USA-20/Wednesday/us-20-Artuso-An-Unauthenticated-Journey-To-Root-Pwning-Your-Companys-Enterprise-Software-Servers-wp.pdf
- Onapsis Threat Report:
  - RECON SAP Vulnerability
  - Cyber Risk Assessment
  - FAQs

VISIT: https://www.onapsis.com/recon-sap-cyber-security-vulnerability

BUSINESS RISK ILLUSTRATION

Ensuring application availability, streamlining audit processes and protecting the business from risk are essential.

OPERATIONAL RESILIENCY ASSESSMENT

Prevent application downtime and costly business disruption

“By automating our change control processes, we saved $3 million by improving code quality and reducing import errors to production.”

- CIO of Global Manufacturing Company

AUDIT EFFICIENCY ASSESSMENT

Eliminate resource consuming manual audit processes

"We automated 92% of the testing and validation of IT controls for Sarbanes-Oxley—saving us over $1 million per year.“

- CFO of Pharmaceutical Company

CYBER RISK ASSESSMENT

Reduce vulnerabilities and misconfiguration to protect the business

"We remediated 75% of our vulnerabilities including all critical ones ahead of a large digital transformation project.“

- CISO of Fortune 500 Biotech Company

onapsis

onapsis

Thank you

Contact:
frederik.weidemann@onapsis.com

onapsis