SAP fixed a flaw in xMII that could□ open the door to nation-state hackers

February 10, 2016 By Pierluigi Paganini

SAP fixed a□ vulnerability affecting SAP MII can be used as a starting point of multi-stage attacks aiming to get control over plant devices and manufacturing systems.

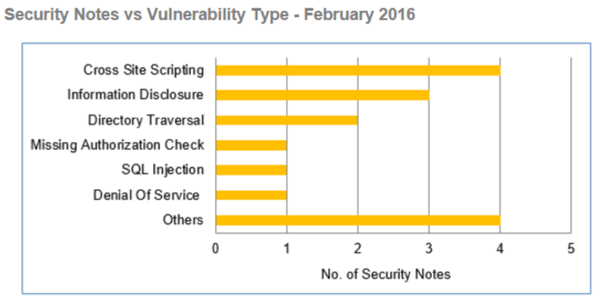
SAP fixed a critical vulnerability in its application□ that could be exploited by hackers, especially nation-state actors, to compromise industrial manufacturing software. SAP issued a critical

Manufacturing Integration and Intelligence (xMII).

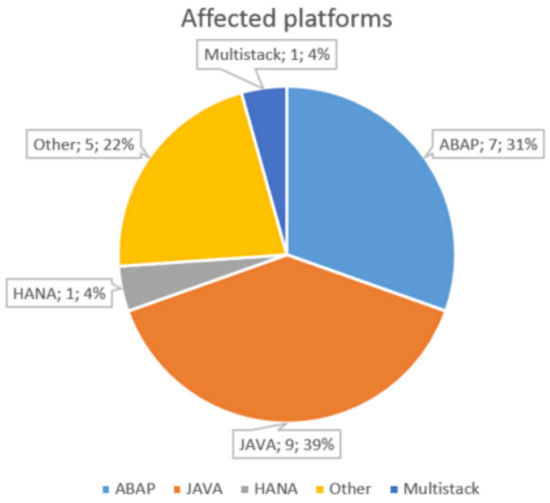
The SAP Manufacturing Integration and Intelligence (xMII) solution implements a sort of software hub that connects ERP software (Enterprise Resource Planning) and other enterprise applications with plant floor and Operational Technology devices□ (OT).

This specific SAP solution is widely adopted in the□ energy industry that is known to be a privileged target for state-sponsored hackers.

SAP published a SAP Security Notes February 2016 – Review and also a summary docs that contains the information on the Patch Day Security Notes that are released on second Tuesday of every month and fix flaws in SAP solutions.□

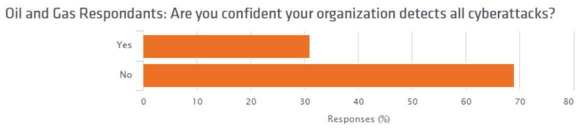

Security Notes vs Vulnerability Type - February 2016

According to data provided by SAP, most of the fixed holes affects SAP NetWeaver's J2EE□ application security, meanwhile Cross Site Scripting represents the principal vulnerability type.


Affected platforms

A study conducted by TripWire in January revealed successful cyber attacks on the energy industry increased as never before in 2015.

Data published in the report confirmed that 69% of respondents to the Tripwire study declared they “weren’t confident” their company would be able to detect every cyber attack.



According to US Department of Homeland Security in 2014 the companies in the energy industries suffered 245 incidents.

The flaw fixed by SAP in the in SAP xMII is a directory traversal vulnerability, hackers could exploit it to penetrate into plant floor and OT networks and launch the attack against the connected ICS and SCADA systems.

The flaw could allow attackers to access the file system of the SAP server with unpredictable consequences.

“

> “Any vulnerability a
> SAP MII can be used
> starting point of mul
> attacks aiming to ge
> over plant devices a
> manufacturing system
> Polyakov Alexander,
> SAP and Oracle secu
> specialists ERPScan,
> Reg Similar “ attack
> scenarios were presented b
> us at the BlackHat
> conference but for th
> gas [industry] in par

Pierluigi Paganini

(Security Affairs – civil nuclear facilities, SAP xMII)

Share it please ...

energy industry

ERP

nation-state hackers

SAP

SAP Manufacturing Integration and Intelligence

xMII

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at□ Bit4Id, firm leader in identity□ management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field,□ he is Certified Ethical Hacker at□ EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led

Pierluigi to find the security blog□ "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone,□ ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Crooks are offering Apple employees up to $23,000 for their login credentials

NEXT ARTICLE

Poseidon Group, a single actor behind a long series of attacks

YOU MIGHT ALSO LIKE

Energy industry under unceasing attack in 2015

January 17, 2016 By Pierluigi Paganini

The ISIL is trying to hack American electrical power companies

October 17, 2015 By Pierluigi Paganini

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in□ identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

[redacted]

Back to top ^