THREAT REPORT

10KBLAZE

Protection From a Cyber Exploit with the Power to Burn Financial Statements

www.onapsis.com

onapsis

Introduction

In April 2019, several new exploits targeting two technical components of SAP® applications were released after being presented in a session at the OPCDE Security Conference. These exploits, dubbed 10KBLAZE, **can lead to full compromise of SAP applications, including deletion of all business application data**, and modification and extraction of highly sensitive and regulated information. They affect applications such as SAP S/4HANA®, SAP Enterprise Resource Planning (ERP), SAP Product Lifecycle Management (PLM), AP Customer Relationship Management (CRM), SAP Human Capital Management (HCM), SAP Supply Chain Management (SCM), SAP Supplier Relationship Management (SRM), SAP NetWeaver® Business Warehouse (BW), SAP Business Intelligence (BI), SAP Process Integration (PI), SAP Solution Manager (SolMan), SAP Governance, Risk & Compliance 10.x (GRC) and SAP NetWeaver ABAP® Application Server 7.0 - 7.52.

These exploits are not targeting vulnerabilities inherent in SAP code, but administrative misconfigurations of SAP NetWeaver installations (including S4/HANA). If these configurations are not secured, as recommended by SAP (easier to do during an implementation and GoLive process), recently published exploits can be used against affected companies.

These exploits can be executed by a remote, unauthenticated (no username and password) attacker having only network connectivity to the vulnerable systems. While the affected technical components are not typically required nor recommended to be exposed to untrusted networks, Onapsis has seen examples of numerous systems having been found to be exposed directly to the internet.

As part of our commitment to protect our customers' business-critical applications and key business data, the Onapsis Research Labs continuously analyzes threats and attack vectors affecting SAP and Oracle applications. Because of the recent public availability of new exploits, Onapsis is releasing this threat report and spearheading a joint effort between several leading security and services organizations to alert SAP customers globally of its potential impact. Additionally, we have released two open source Snort signatures to provide all SAP customers a detection mechanism that can be used to monitor system risk while misconfigurations are being addressed.

Delivering on our commitment to our mutual customers, this threat report serves as a guide to help you understand if your system is exposed and provide you with risk mitigation information to ensure that your organization's system is protected.

Risk and Business Impact

SAP NetWeaver is one of the most widely deployed platforms developed by SAP, running most of the business-critical processes that companies depend on such as payroll, sales, invoicing, and manufacturing, among others. In this threat report, the Onapsis Research Labs describes how most global SAP implementations may be vulnerable to this full-system compromise attack vector and how you can mitigate this in your organization.

SAP NetWeaver installations, if misconfigured, can be compromised by attackers using these exploits. Based on publicly available data provided by SAP[1], Onapsis estimates that approximately 50,000 companies and a collective 1,000,000 systems are currently using SAP NetWeaver and S/4HANA. Onapsis research gathered over ten years calculates that nearly 90% of these systems, approximately 900,000, may suffer from the misconfigurations for which these exploits are now publicly available.

The impact and risk to businesses created by these critical exploits include attackers creating new users in the SAP system with arbitrary privileges, allowing them to view and modify critical and sensitive business data (e.g., employees' personal information, financial statements, banking transfer and routing processes, patient health records, critical infrastructure and energy distribution schedules, medication dosage amounts). Attackers can also leverage these exploits to perform arbitrary business functions such as creating new vendors or purchase orders, modifying bank accounts and releasing payments, gaining full access to SAP databases, taking SAP systems offline or permanently deleting business-critical and regulated information. **In summary, all confidentiality, integrity, and availability of the data stored in these systems and corresponding databases are vulnerable to this exploit.**

This further demonstrates the need for organizations to build a governance program involving Information Security, SAP, and Internal Audit teams to take ownership for the security of their SAP implementations. Companies should no longer rely solely on Segregation-of-Duties and GRC to manage security, but need to expand to vulnerability and configuration management, patch management and continuous monitoring of these systems.

[1] SAP TechED session SEC809: 44,000 SAP ERP 6.0 implementations (October 2018), SAP Corporate fact sheet: More than 10,000 S/4HANA Customers (Q1 2019)

Chronology

of Onapsis involvement with SAP Gateway and Message Server Misconfigurations

2005
SAP releases SAP Security Note #821875[2] "Security Settings in the Message Server" with details on how to properly set up an access list for Message Server

2007
Onapsis CEO Mariano Nunez discovers Gateway attacks and hosts the first public presentation about cyber threats affecting SAP applications at Black Hat

2009
SAP releases SAP Security Note #1408081[3] "Basic Settings for Reg_info and Sec_info" detailing how to properly configure the access list for SAP Gateway

2010
SAP releases SAP Security Note #1421005[4] "Secure Configuration of the Message Server" where it reinforces the relevance of properly configuring Message Server ACL

2011
SAP releases Kernel 7.20, including the keyword *internal* for ACLs, allowing automatic identification of application servers in the access list for the SAP Gateway

2016
Onapsis identifies a potential new attack vector and reports it to SAP, who states that the attack is not possible if SAP Security Note #1421005[5] is properly implemented

2017
Onapsis evaluates SAP implementations and detects that 9 out of 10 SAP systems could be compromised through this new attack vector

DECEMBER 2017
Onapsis reaches out to customers to ensure they have fixed the configuration and addressed the risk in their existing landscapes, through our Advanced Threat Protection service

APRIL 2018
Onapsis publishes a threat report to give all SAP customers the information they need to mitigate this critical risk

APRIL 2019
Exploits are made available to the public during OPCDE Conference in Dubai

[2] https://launchpad.support.sap.com/#/notes/821875
[3] https://launchpad.support.sap.com/#/notes/1408081
[4] https://launchpad.support.sap.com/#/notes/1421005
[5] https://launchpad.support.sap.com/#/notes/1421005

Technical Details

GENESIS: SAP GATEWAY ACL AND REMOTE COMMAND EXECUTION

In 2007, Onapsis CEO Mariano Nunez presented at Black Hat Europe[6] on the topic of cyber threats to SAP systems through the RFC protocol. In his presentation, the Onapsis co-founder detailed how an attacker can execute remote OS commands through unprotected RFC Gateways. This presentation was the foundation for an increasing focus on SAP cybersecurity, including the number of SAP Security Notes published by SAP[7], and for the whole business-critical application security industry.

In 2012, SAP released SAP NetWeaver Application Server 7.31, where the SAP Gateway access list is secure by default, by adding specific (and secure) configurations. By the end of that year, SAP presented at SAP TechEd, "SAP Runs SAP – Remote Function Call: Gateway Hacking and Defense." They stressed that, "**unprotected RFC gateways allow manipulation of business processes in SAP systems**,"[8] including full control over SAP systems bypassing any other SAP security controls, manipulation of data which endangers legal compliance, data theft or event unavailability of data and systems.

OLD AND NEW THREAT: SAP MESSAGE SERVER ACL

The SAP Gateway ACL files are now delivered in a secure mode by default on every new SAP implementation, but there are other SAP services that share a similar protection scheme through Access Control Lists (ACL), and one of them is the SAP Message Server. Any SAP Application Server must be registered within the SAP Message Server in order to be able to serve the users on time and perform load balancing. The following image illustrates the registration process:

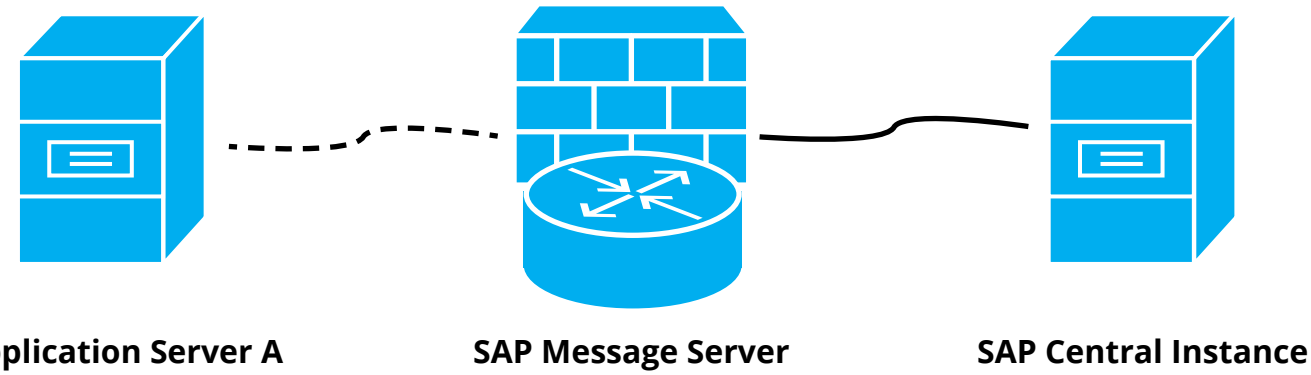

Figure 1: SAP Message Server Service and its Connection to Application Servers

[6] http://sapvod.edgesuite.net/TechEd/TechEd_Vegas2012/pdfs/SIS203.pdf
[7] https://www.onapsis.com/blog/sap-security-notes-2016-year-review
[8] http://sapvod.edgesuite.net/TechEd/TechEd_Vegas2012/pdfs/SIS203.pdf

The SAP Message Server implements a protection mechanism, also known as an ACL, to check which IP addresses can register an application server and which ones cannot. This ACL is controlled by the profile parameter *ms/acl_info*. This parameter should contain a path to a file with the following format:

HOST=[*| ip-adr | hostname | Subnet-mask | Domain] [, ...]

Figure 2: SAP Message Server Service ACL Configuration

Details on how to properly configure this access file were published by SAP in 2005 through SAP Security Note #821875[9] "Security Settings in the Message Server" with information on how to properly set up an ACL for the Message Server. Nevertheless, this parameter is set with default configuration, as well as the ACL content open, **allowing any host with network access to the SAP Message Server to register an application server in the SAP system.**

The registration process is performed using the Message Server internal port 39<xx> (3900 by default). As explained in the SAP Security Note #1421005[10], this port should be secured and only accessible by trusted application IP addresses.

If the SAP system lacks a secure Message Server ACL configuration, an attacker can exploit this misconfiguration and register a fake Application Server in the SAP system. An attacker only needs to be able to "speak" the message server protocol to register a fake Application Server. This could lead to a full system compromise through more complex attacks such as a Man-in-the-Middle attack, where an attacker could steal user credentials acting as an Application Server. Additionally, attackers could shut down the SAP system or even achieve full system compromise with a fake server registration.

[9] https://launchpad.support.sap.com/#/notes/821875
[10] https://launchpad.support.sap.com/#/notes/1421005

Assess, Detect & Prevent

Since this is a risk based on misconfigurations for access lists that are **present in almost any SAP implementation in the world, and may not be easily secured**, below is a summary of how to define if you are at risk, understand exposure, monitor for attacks and then remediate if there is any risk.

Onapsis customers have the ability through the Onapsis Security Platform (OSP) to mitigate this risk by:

- **Determining their level of exposure through the assessment feature**
- **Monitoring and detecting possible attacks using these exploits while misconfigurations are being addressed**
- **Adjusting configurations and locking them in place to prevent exposure in the future**

Based on the criticality of this attack and the publication of the exploits, we offer guidelines in this threat report. For companies that are not OSP customers, we offer a free assessment to quickly determine whether they are vulnerable or not to this attack.

Visit us at **www.onapsis.com/10kblaze** for more information.

ARE YOU AFFECTED?

In order to check if your systems are secure against 10KBLAZE, follow the below steps for each server.

MESSAGE SERVER

These components are critical to SAP applications and ACLs should be properly configured, according to SAP Security Note #1421005, to avoid risk.

In **ABAP-based servers**, you can use SAP GUI with a privileged/admin account and:

1. Execute transaction SMMS
2. Click on menu item "Goto -> Security Settings -> Access Control -> Display"
3. Check that this file has a restrictive ACL allowing access only to the required application servers, according to the business requirements

For **JAVA servers**, the ACL file is usually located in the folder: /usr/sap/<SID>/SYS/global/ms_acl_info. Contact your SAP team, consultant or Onapsis for more information.

GATEWAY

The starting of external RFC servers is restricted through the *gw/sec_info* profile parameter. This parameter points to an ACL text file that should be configured in order to prevent unauthorized connections. Since the launch of SAP NetWeaver Application Server 7.31, the SAP Gateway access list is secure by default, but you need to ensure that this configuration has not drifted into an insecure state.

In order to check the Gateway ACL file, you can use SAP GUI with a privileged/admin account and:

1. Execute transaction SMGW
2. Click on menu item "Goto"->"Expert Functions"->"External Security"-> "Display (Sec Info)"
3. Check that these files apply a restrictive ACL, allowing only trusted servers (USER-HOST) to start RFC servers

FIVE QUESTIONS FOR INFOSEC TEAMS

If you are part of the CISO organization, you may not have a deep understanding of the SAP environment and its complexity. To effectively work with the SAP BASIS team, it is necessary to better understand if your company is at risk.

Here are 5 questions to ask the BASIS or SAP experts in your organization:

1. Do we have a list of SAP Gateway and SAP Message Server systems?
   - If **no**, create one
2. Are any of our systems exposed to external networks?
   - If **yes**, risk to the organization may be increased
3. Do we run SAP NetWeaver Application servers versions below 7.31?
   - If **yes**, risk may be increased and your organization will need to apply the appropriate SAP Security Notes
4. Have we secured the SAP Message Server Access List from its default value?
   - If **no**, you are at risk no matter how secure your Gateways are
5. Is there any threat monitoring tool for SAP servers?
   - If **no**, you won't be alerted if someone tries to use these exploits

DETECT: IS SOMEONE RUNNING THESE EXPLOITS IN MY ENVIRONMENT?

If you are at risk, moving to a secure configuration state may take time. Properly monitoring your SAP environment for attacks and alerts is a best practice, but while securing your systems and beyond, it is recommended to monitor specifically for the execution of these exploits on the network.

Based on the publication of these exploits, Onapsis has decided to release two open source Snort rules in order to help customers properly monitor this threat:

- The first rule matches to the execution of these public exploits - this rule can be implemented immediately, since there is no reason to have this code running on the network
- The second rule, with a more generic detection, includes monitoring for the payload on the network - since this activity may not be malicious between SAP App Servers, it can only be implemented if a whitelist of IP addresses or network segments can be configured

The Onapsis Snort signature is available on the Onapsis website at https://www.onapsis.com/10kblaze.

SAP Gateway rules are two of over one thousand detection signatures that the Onapsis Research Labs have added to the Onapsis Security Platform. Onapsis customers do not need to include Snort rules if SAP servers are properly linked to OSP, including an alert if SAP Message Server App Servers registration is detected (this is a previous and necessary step to exploit the Gateway if ACLs are secure).

Onapsis is working with recognized firewall providers to help them release signatures for this attack in their products as well. While being able to detect these attacks is a great first step, organizations can only truly be secure if they take the time to implement the SAP Security Notes. The monitoring can be used as a compensating control to help organizations are they are securing these misconfigurations.

PREVENT: SECURE YOUR SAP ENVIRONMENT

Invest in prevention technology and processes to lock down secure configurations in your systems. If you are at risk, you need to implement secure configurations in both SAP Message Server and SAP Gateway. As a summary, the **access list in all the servers should be configured in a secure way**.

Some other configurations should be also addressed to fully secure the environment. For example, to fully secure Message Server, we recommended to avoid using *admin port* (or use it restricted for specific network segments). The following SAP Security Notes describe the steps:

- SAP Security Note #1408081 "Basic Settings for Reg_info and Sec_info" (2009), details how to properly configure the access list for **SAP Gateway** (which, as mentioned before, is secure by default since version 7.31)
- SAP Security Note #821875 "Security Settings in the Message Server" (2005), explains how to properly configure **Message Server** ACL; it was later reinforced with SAP Security Note #1421005 (2010)

WARNING: Before applying the changes in a productive system it is highly recommended to analyze interfaces currently in use in order to avoid disrupting existing processes.

Remediation should be part of a program that helps bridge the gap between teams: Align IT Security, Internal Audit, BASIS and SAP Security teams towards the unified goal of running secure SAP applications. This program should include:

1. Visibility: Properly configure SAP Message Server ACL. SAP published instructions for this more than ten years ago, which confirms the need for more investment and education in SAP cybersecurity if this vulnerability is still present in your systems.
2. Continuous monitoring and compliance checks: Validate that security-relevant configurations such as the Message Server ACL files do not change the security posture of the entire system.
3. Prevent: Manage configuration drift through technology and processes so once you secure your configuration, changes made inadvertently or without awareness of risk, do not render it insecure again. For OSP customers, Enforce & Protect capabilities can be used to log, alert and lock down to avoid configuration drift. Once everything is securely configured, OSP ensures it does not move to an insecure state again.

References

- CWE-284: Improper Access Control
  https://cwe.mitre.org/data/definitions/284.html

- SAP Security notes in the SAP Launchpad

About Onapsis Research Labs™

SAP and Oracle Security Threat Intelligence is produced by the Onapsis Research Labs, a team of leading security experts who combine in-depth knowledge and experience to deliver technical analysis with business context and provide sound security judgment to the market. The team works closely with SAP and Oracle product security teams to responsibly deliver the information to customers and has released over 150 advisories to date, with over 100 affecting Oracle EBS; has consulted on impact with over 180 Onapsis enterprise customers; and regularly presents at leading security, Oracle and SAP conferences around the world. Onapsis was the first to deliver "SAP Security In-Depth" publications that provide detailed analysis on security risks impacting SAP and SAP HANA and are now the first to deliver "Oracle Security In-Depth" publications focusing solely on Oracle application security.

About Onapsis

Onapsis helps organizations be cyber resilient by protecting their business-critical applications, keeping them compliant and safe from insider and outsider threats. Our patented solutions are used to accelerate digital transformation initiatives – including transitioning to the cloud – by providing actionable intelligence, continuous monitoring and automated governance for ERP, CRM, PLM, HCM, SCM, BI and cloud-based business-critical applications.

As the proven market leader, global enterprises trust Onapsis to help modernize and strengthen their SAP and Oracle E-Business Suite applications, and to make sure security, IT, DevOps and compliance teams are best prepared for the business needs of the future.

Headquartered in Boston, MA, and with global operations, Onapsis proudly serves more than 300 of the world's leading brands and organizations, including many of the Global 2000. Through our unique strategic alliances with leading consulting and audit firms such as Accenture, Deloitte, IBM, Infosys, PwC and Verizon, Onapsis solutions have become the de facto standard in helping organizations protect what really matters.

For more information, visit us at **www.onapsis.com** or connect with us on **Twitter** or **LinkedIn**.

onapsis