

Alerts and Advisories

Whitepaper

January 2024

© 2024 Software AG. All rights reserved.

Software AG

Table of Contents

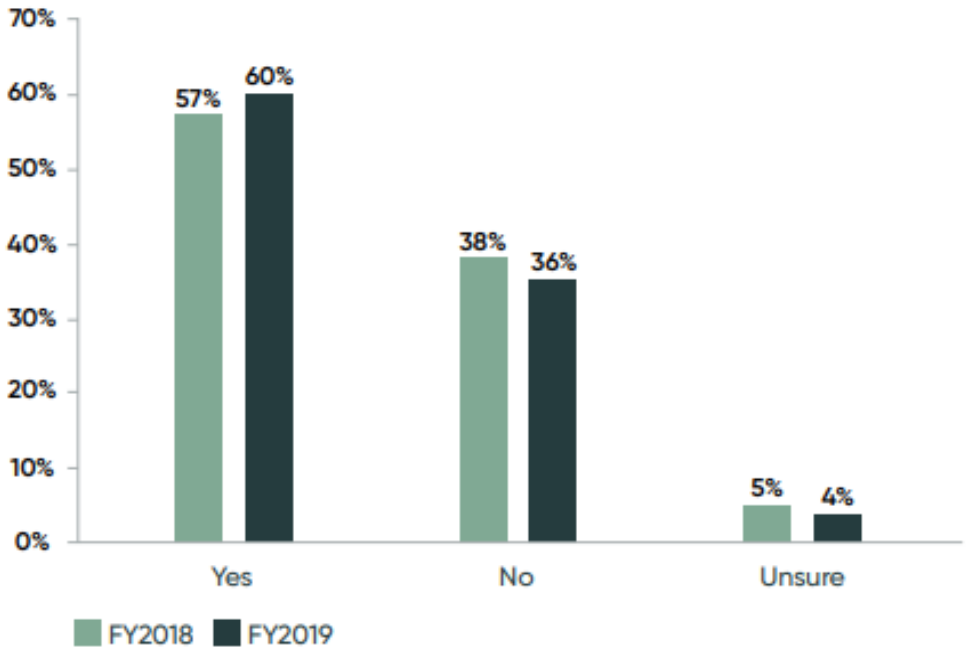
Sl. No.	Section	Page No.
1	Introduction	3
2	Alerts and Advisories	4
3	Publishing Timelines	5
4	Alerts Overview	5
5	Subscription to Early Warnings	7
6	Feedback	8

1 Introduction

As we move forward in today's digital era, we continue to experience an influx of more robust and sophisticated technologies which are being conceived to resolve complex real-world problems. With the introduction and exponential rise in newer technologies and frequent major and minor releases, the crucial task of identifying potential threats and vulnerabilities that may plaque both the existing and new systems alike continues to be recognized as a non-negotiable goal that every organization has prioritized. Hence, securing assets and infrastructure remain imperative to any organization for decades to follow.

According to a survey conducted in 2021, application vulnerability continues to be the most common external attack method. As the number of security vulnerabilities continue to rise, it is important that organizations and its stakeholders remain vigilant, and keep their systems patched and upgraded. Patching is essentially a way to secure software, servers, and technology to maintain operational efficacy. Hence, patch management becomes a critical part of the vulnerability management process that organizations must uphold and embody.

From the survey conducted by ServiceNow on the vulnerability patch management, it was found that *'60% of Breaches in 2019 Involved Unpatched Vulnerabilities'.* The figure below shows the results for the question: *Did any of these breaches occur because a patch was available for a known vulnerability but not applied?'*



In another survey conducted by security company Tripwire**,** they found that - "***IT security professionals admit that one in three breaches are the result of vulnerabilities that they should have already patched***" and "***One in three IT professionals (34%) in Europe***

admitted that their organization had been breached as a result of an unpatched vulnerability (higher than the average of 27%)"

To keep their organizational systems safe, customers must be cognizant of security events and their implications. To that end, Software AG publishes relevant information in the form of subscriptions called Alerts and Advisories process.

2 Alerts and Advisories

The Alerts and Advisories process has been ideated and designed to act as a vital channel of communication between Software AG and its customers regarding every aspect of security pertaining to the organization and its complete range of products.

Software AG recommends that customers manually subscribe to security alerts service on the Empower portal. Only upon subscription will customers be able to avail this service as it is not a default feature. Upon subscribing to this service, customers receive "early warnings or alerts" updating them on the availability of fixes for vulnerabilities reported in Software AG products. By extension, the advisory section of the same document further helps broaden the information spectrum available to the customer regarding the fix and the issue that it is addressing. Security advisories has no subscription, these advisories are published on Empower under the security section - https://empower.softwareag.com/Products/default.aspx?err=Sorry,%20you%20must%20be%20logged%20in%20to%20view%20this%20page.&origin=/Products/Security/default.aspx

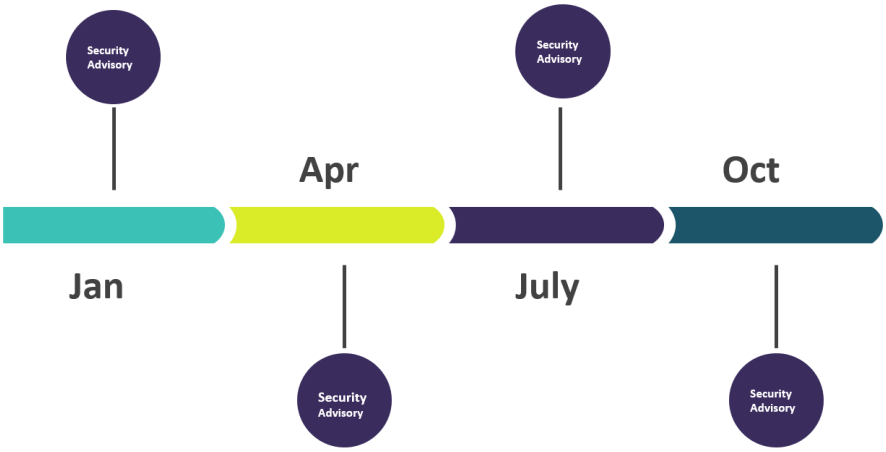
Security advisories are published on critical zero-day vulnerability about the impact on Software AG products, whereas security alerts are quarterly updates to the customers regarding the security fix and a brief description of the vulnerability it addresses. The customer must log in to the Empower to view these advisories.

These alerts are delivered to the subscribed customers through two channels of communication – email and Empower portal. To view these alerts and advisories documents on Empower, the customer must login using their Empower credentials and navigate to the "Early Warnings/ Critical Alerts" section under "Knowledge Centre". The subscription to the security alerts can be managed under the "Subscribe to knowledge Centre" section.

Security alerts are published every quarter starting from January. In this process, the security vulnerabilities fixes are reviewed, and the respective patch details are retrieved. Later, a document is prepared composing different aspects encompassing these details. In situations where critical security events occur that may threaten or completely disrupt the operational functionality of any product, then this initiates an early response from the team at Software AG overlooking these matters.

3 Publishing Timelines

Security advisories are published every quarter starting from January.



4 Alerts Overview

Every quarter, the security vulnerabilities fixes are reviewed, and the respective patch details are retrieved. Later, a document is prepared composing of different aspects as indicated below:

4.1 Alerts header

The advisory header contains details about the product and version. It also specifies the operating system for which the fix is applicable.

Early Warning - NUM_107_EarlyWarning_001

Product:	Software AG Universal Messaging (NUM)
Version	10.7
Last Updated:	17 . Aug 2021, 08:08

Doc ID:	500482
Operating System Family:	ALL
Operating System:	Any Operating System

4.2 Advisory Body

The advisory body gives more insights about the issue and fix details.

- Announced: The day the advisory was announced.
- Affects: The product name for which the stated fix is applicable.

- Severity: This field is about the risk rating levels.
- Description: This gives information about the security issue being fixed and the CVE details.
- Impact: This explains the repercussions.
- Workaround: If there is no fix available then a workaround is stated.
- Fix: This gives information about the fix to be applied

Early Warning Details:

Early Warning regarding the security fixes provided by NUM_10.7_wM_Client_Fix1

Announced: 2021-08-17

Affects: WebMethods Universal Messaging 10.7

Severity: High

I. Description
The below mentioned security issue(s) are addressed in the above mentioned fix NUM_10.7 _wM_Client_Fix1. However, we suggest you upgrade to the latest fix available which includes the above mentioned fixes as well as other latest updates.

Security vulnerabilities were discovered in OpenSSL version 1.1.1f

The issue is resolved. The OpenSSL version used in Universal Messaging has been upgraded from 1.1.1f to 1.1.1g. Reference: CVE-2020-1967.

II. Impact
Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or an unrecognized signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. The issue did not affect OpenSSL prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected: 1.1.1d-1.1.1f).

III. Workaround
NA

IV. Fix
NUM_10.7_wM_Client_Fix1

4.3 Contact details

This section gives information about contacting Software AG personnel on further assistance.

VI. Contacting Us
If you have any questions about this alert or need to report an additional issue you may send an email to the Software AG security team:
Email: [security@softwareag.com | mailto: security@softwareag.com]

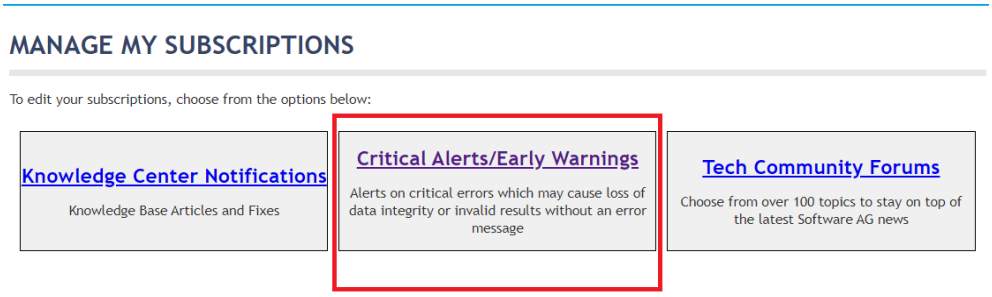
Authorized technical support contacts can reach Software AG Global Support in the following ways:
Web: https://empower.softwareag.com/eservice/default.asp (online support center)

You can find complete contact information in our Global Support Contact Directory at
https://empower.softwareag.com/public_directory.asp

You can also participate in our Software AG Developer Communities, which feature technical information, useful resources, and online discussion forums, moderated by Software AG professionals, to help you do more with technology:
http://www.softwareag.com/Corporate/community/dev_net/default.asp

5 Subscription to Early Warnings

The subscription to the security alerts can be managed on Empower under " Knowledge centre" → " Subscribe to knowledge Centre". If you are subscribed to early warnings for your product, you would receive the security advisories as well. You can manage your subscription by logging in to Empower .



We can never overlook the role security plays in strengthening the relationship and trust between an organization and its customers. It would be futile to underplay its undeniable significance in the cultivation of trust and confidence in an organization's ability to deliver safe and reliable products and services to its customers.

6 Feedback

Software AG welcomes your feedback on this whitepaper. If you have any comments, please drop an email to security@softwareag.com.

ABOUT SOFTWARE AG

The digital transformation is changing enterprise IT landscapes from inflexible application silos to modern software platform-driven IT architectures which deliver the openness, speed and agility needed to enable the digital real-time enterprise. Software AG offers the first end-to-end Digital Business Platform, based on open standards, with integration, process management, in-memory data, adaptive application development, real-time analytics and enterprise architecture management as core building blocks. The modular platform allows users to develop the next generation of application systems to build their digital future, today. With over 50+ years of customer-centric innovation, Software AG is ranked as a leader in many innovative and digital technology categories. Learn more at www.SoftwareAG.com.

© 2024 Software AG. All rights reserved. Software AG and all Software AG products are either trademarks or registered trademarks of Software AG. Other product and company names mentioned herein may be the trademarks of their respective owner