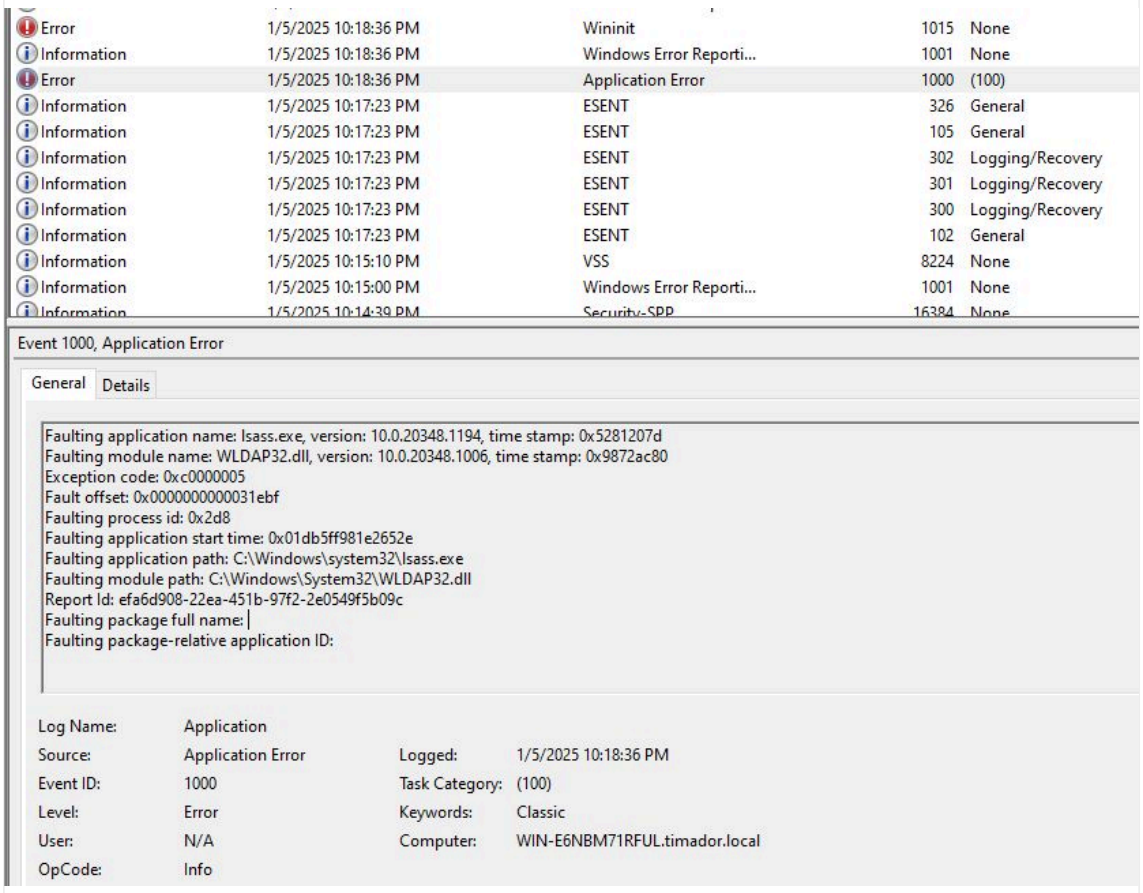
Post de Travis Green

Travis Green
Cybersecurity Researcher | CISSP, GCIA, CCSP
2 mois

If you're looking for evidence of CVE-2024-49113 #ldapnightmare in system logs, search for event ID 1000 containing WLDAP32.dll:

Faulting application name: lsass.exe, version: 10.0.20348.1194, time stamp: 0x5281207d
Faulting module name: WLDAP32.dll, version: 10.0.20348.1006, time stamp: 0x9872ac80

Full event exports here: https://lnkd.in/gR7J7hYR



612 · 19 commentaires

J'aime Commenter Partager

Harlan Carvey 2 mois
Staff Threat Intel Analyst, Adversary Tactics

My hope is that one day, we can begin using more accurate nomenclature for these things.

"system logs"? It's the Application Event Log. A Windows system can have hundreds of "system logs", one of which is the System Event Log. However, the name of the log file provides insight into it's content, and the screen shot does not show a record from the System Event Log.

Event IDs are not unique, especially in the Application Event Log. There can be multiple different records with the same event ID...I've seen event IDs such as "0", "1", "100", etc., used between different applications. There are two different records for event IDs 4624 and 4625, respectively. So, let's use the event source and ID for specificity and context.

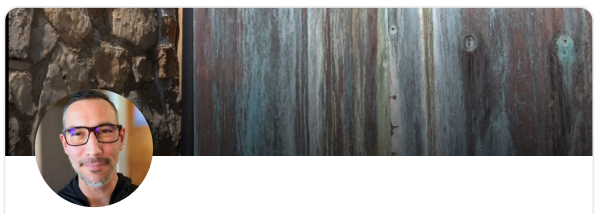
J'aime · Réagir | 11 réactions

Florian Roth 2 mois
VP R&D at Nextron Systems

Could someone write a Sigma rule and create a PR on our public repo - because this information is gold but not actionable. (I'm still on vacation and could only take care of it after the trip)

J'aime · Réagir | 12 réactions

Huy Kha 2 mois
Senior Identity & Security Architect @ Semperis



2 153 abonnés
68 posts
Voir le profil + Suivre

Explorer les sujets

Vente
Marketing
Services informatiques
Administration des affaires
Gestion des ressources humaines
Ingénierie
Compétences générales
Tout voir

Have you already enabled Postmortem debugging with ProcDump of WER and captured the crash of lsass? With that dump file, you can then display the crashing call stack which may be useful as well

J'aime · Réagir | 2 réactions

David G. 2 mois
CISSP | RHCA V | CCSP | CSSLP | CK{A,AD,S} | CEH Master | Security+ | LPI3 & 303 | AWS | Dev...

Nice tip

J'aime · Réagir | 2 réactions

Ilan Duhin 2 mois

Amazing tip

J'aime · Réagir | 1 réaction

Muhammad Hasnain 2 mois
Red Teamer|Penetration Tester|Vulnerability Assessment|CTF Player

Hassnain J.

Herb S. 2 mois
Certified Azure Security Architect @ Microsoft | CISSP, CCSP

Excellent work Travis

J'aime · Réagir | 1 réaction

Will Jackson 2 mois
Cybersecurity Incident Commander for a US Government agency

Excellent work Travis

J'aime · Réagir | 1 réaction

Voir plus de commentaires

Plus de posts pertinents

CVE Find
180 abonnés
5 mois

[CVE-2024-7098: CRITICAL] Improper Restriction of XML External Entity Reference vulnerability in SFS Consulting ww.Winsure allows XML Injection.This issue affects ww.Winsure: before 4.6.2.
https://lnkd.in/gyZXrqjs

J'aime Commenter Partager

Andrew Butenko
7 mois

Interesting discovery by results of today's work:
I was applying changes to the form of the entity and I got an error "Error: We ran into a problem publishing the form. Please try again. ..."
I checked the network traffic for an error occurring and found the following error:
Property [Property Name] is not declared in the control manifest. More Details:Parent Type:SystemForm;SubType:main;Parent Id:923c942a-2189-ec11-93b0-0022482b2cb9;Associated entity:[Entity Name];Control Description Xml:Unexpected schema;Control Reference Xml:Unexpected schema;Error Message:-2146041800;Additional Information:;

So the reason was that the current version of **#PCF** control has more required privileges than when PCF control was initially added to the form.

The fix was obvious - open the mentioned control, provide a value for the missing property, save, publish, and voila - the error goes away.

48 · 1 commentaire

J'aime **Commenter** **Partager**

Identifiez-vous pour afficher ou ajouter un commentaire

Olle E Johansson
7 mois

The Package URL is the favourite replacement for the CPE in vulnerability databases. For software that isn't distributed as packages or containers - commercial software, open source that is distributed in source code format (typically .tgz) a SWID PURL identifier works well. Test the PURL SWID generator for your software!

https://lnkd.in/d7zbrSWC

#PURL #SBOM #CYCLONEDX #SPDX
OWASP CycloneDX SBOM/xBOM Standard SPDX SBOM

26 · 1 commentaire

J'aime **Commenter** **Partager**

Identifiez-vous pour afficher ou ajouter un commentaire

Anjan Roy
Senior Cryptography Engineer at Cryptography Research Center, TII, Abu Dhabi
1 ans

Just finished adding timing leakage detection tests (using dudect), along with ASAN (address sanitizer) and UBSAN (undefined behaviour sanitizer) builds for property based tests of my C++20 library implementation of Ascon cipher suite !

Ascon is being standardized by NIST as light-weight cipher suite, used for encryption, hashing and authentication 🥳

Good news is that I've found zero issues in my library implementation 😌

https://lnkd.in/ez2hDs4r

Add Extensive Testing by itzmeanjan · Pull Request #24 · itzmeanjan/ascon
github.com

3

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

HTMD Community
3 180 abonnés
10 mois

[New Post] 🦹‍♂️ ♌ Fixed ConfigMgr SMS_SERVICE_CONNECTOR Issue -
https://lnkd.in/gEhgwq8G
⏩ SCCM SMS_SERVICE_CONNECTOR Issue
⏩ Failed to download entity Policy
⏩ Issue Fixed?
#SCCM #ConfigMgr #MSIntune #HTMDCommunity

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Hernan Espinoza
Profesional en Agencia Nacional de Ciberseguridad de Chile
10 mois

CVE-2024-32962 - CVSS 10.0 - EPSS 0.04% - xml-crypto is an xml digital signature and encryption library for Node.js. In affected versions the default configuration does not check authorization of the signer, it only checks the validity of the signature per section 3.2.2 of the w3 xmldsig-core-20080610 spec. As such, without additional validation steps, the default configuration allows a malicious actor to re-sign an XML document, place the certificate in a <KeyInfo /> element, and pass xml-crypto default validation checks. As a result xml-crypto trusts by default any certificate provided via digitally signed XML document's <KeyInfo />. xml-crypto prefers to use any certificate provided via digitally signed XML document's <KeyInfo /> even if library was configured to use specific certificate (publicCert) for signature verification purposes. An attacker can spoof signature verification by modifying XML document and replacing existing signature with signature generated with malicious private key (created by attacker) and by attaching that private key's certificate to <KeyInfo /> element.
Ref.1: https://lnkd.in/efN5yFXJ

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Peter Bishop
Software Engineer [React, SwiftUI, Flutter, Node]
2 mois

#webhooks, #signatureverification SHA256 Webhook Signature Verification is surprisingly simple! When you create a web hook that supports this a secret will be generated for it. Use that in combination with the request body (the payload) to generate a SHA256 hash value to compare with the signature sent with the payload to verify the data is legit.

2

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

CVE Find
180 abonnés
3 mois

[CVE-2024-52442: CRITICAL] Incorrect Privilege Assignment vulnerability in Userplus UserPlus allows Privilege Escalation.This issue affects UserPlus: from n/a through 2.0.
https://lnkd.in/emXVPHR5

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire