

GitHub Gist

Search...


All gists

Back to GitHub

Sign in

Sign up

Instantly share code, notes, and snippets.



travisbgreen / CVE-2024-49113.md

Secret

Star 1

Fork 1

Created 2 months ago

<> Code

Revisions 1

Stars 1

Forks 1

Embed

<script src="https://"

Download ZIP

CVE-2024-49113 event log

<> CVE-2024-49113.md

Raw

Log Name: Application

Source: Application Error

Date: 1/5/2025 10:18:36 PM

Event ID: 1000

Task Category: (100)

Level: Error

Keywords: Classic

User: N/A

Computer: WIN-E6NBM71RFUL.timador.local

Description:

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

Exception code: 0xc0000005

Fault offset: 0x0000000000031ebf

Faulting process id: 0x2d8

Faulting application start time: 0x01db5ff981e2652e

Faulting application path: C:\Windows\system32\lsass.exe

Faulting module path: C:\Windows\System32\WLDAP32.dll

Report Id: efa6d908-22ea-451b-97f2-2e0549f5b09c

Faulting package full name:

Faulting package-relative application ID:

Event Xml:

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">

<System>

<Provider Name="Application Error" />

<EventID Qualifiers="0">1000</EventID>

<Version>0</Version>

<Level>2</Level>

<Task>100</Task>

<Opcode>0</Opcode>

<Keywords>0x80000000000000</Keywords>

<TimeCreated SystemTime="2025-01-06T05:18:36.2074297Z" />

<EventRecordID>6769</EventRecordID>

<Correlation />

<Execution ProcessID="0" ThreadID="0" />

<Channel>Application</Channel>

<Computer>WIN-E6NBM71RFUL.timador.local</Computer>

<Security />

</System>

<EventData>

<Data>lsass.exe</Data>

<Data>10.0.20348.1194</Data>

<Data>5281207d</Data>

<Data>WLDAP32.dll</Data>

<Data>10.0.20348.1006</Data>

<Data>9872ac80</Data>

<Data>c0000005</Data>

<Data>0000000000031ebf</Data>

<Data>2d8</Data>

<Data>01db5ff981e2652e</Data>

<Data>C:\Windows\system32\lsass.exe</Data>

<Data>C:\Windows\System32\WLDAP32.dll</Data>

<Data>efa6d908-22ea-451b-97f2-2e0549f5b09c</Data>

<Data>

```
</Data>
<Data>
</Data>
</EventData>
</Event>
```

```
Log Name:      Application
Source:        Microsoft-Windows-Wininit
Date:          1/5/2025 10:18:36 PM
Event ID:       1015
Task Category: None
Level:         Error
Keywords:      Classic
User:          N/A
Computer:      WIN-E6NBM71RFUL.timador.local
Description:
A critical system process, C:\Windows\system32\lsass.exe, failed with status code c0000005. The machine must now
Event Xml:
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Wininit" Guid="{206f6dea-d3c5-4d10-bc72-989f03c8b84b}" EventSourceName="Wininit" />
    <EventID Qualifiers="49152">1015</EventID>
    <Version>0</Version>
    <Level>2</Level>
    <Task>0</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8000000000000000</Keywords>
    <TimeCreated SystemTime="2025-01-06T05:18:36.4575296Z" />
    <EventRecordID>6771</EventRecordID>
    <Correlation />
    <Execution ProcessID="0" ThreadID="0" />
    <Channel>Application</Channel>
    <Computer>WIN-E6NBM71RFUL.timador.local</Computer>
    <Security />
  </System>
  <EventData>
    <Data>C:\Windows\system32\lsass.exe</Data>
    <Data>c0000005</Data>
  </EventData>
</Event>
```

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

