Assignment 3.1: Secure Software Development Life Cycle (SSDLC) - Microsoft & Mac

Joshua A. Wortz

University of San Diego

CSOL-560

Dr Varma

11/14/2025

Security cannot be treated as a post-deployment consideration in modern software development. Microsoft's Security Development Lifecycle (SDL) embeds security requirements, threat modeling, verification, and monitoring into every phase of product development (Microsoft, 2024). Windows 11 demonstrates these principles through integrated audit logging, secure authentication flows, automated diagnostics, and application health reporting.

This paper evaluates these lifecycle principles on a live Windows 11 system by examining Security, System, and Reliability Monitor logs. These findings are contextualized through Microsoft's Operational Security Assurance (OSA) model and aligned with ISO 27001:2013 Annex A controls and the NIST Cybersecurity Framework (CSF). By analyzing real events, this paper demonstrates how SDL drives secure operation, detection, and resiliency, and how system telemetry and auditability reinforce secure development practices after deployment.

Microsoft SDL and Operational Security Assurance

The Microsoft SDL mandates secure-by-default configuration, minimized attack surface, threat modeling, continuous monitoring, and rapid response processes (Microsoft, 2023). Two practices particularly relate to logging:

1. Secure by Default

Under SDL, systems ship with hardened defaults, including minimized services, disabled optional components, and reduced exposure (Xiang et al., 2025). In practice, this explains why components such as AppLocker, IIS, and SQL logging were not present on the evaluated system.

2. Continuous Monitoring

SDL requires systems to include comprehensive audit logging, event correlation, and rapid detection capabilities. Research continues to show the role of logging in detecting authentication misuse, driver vulnerabilities, and application instability (Monzani et al., 2026; Yan et al., 2024).

Microsoft's Operational Security Assurance (OSA) operationalizes SDL in production environments by requiring security monitoring pipelines, audit trails, automated alerting, and post-incident investigation support (Microsoft, 2024). Windows 11 incorporates several OSA-aligned elements, including Event Viewer telemetry, reliability analysis, and authentication auditing.

Windows 11 Log Findings

Below are the summaries of the log findings.

Full detailed logs appear in Appendices A–E, each starting on its own page.

Findings Summary

Security Log – Event ID 4624 (Successful Logon)

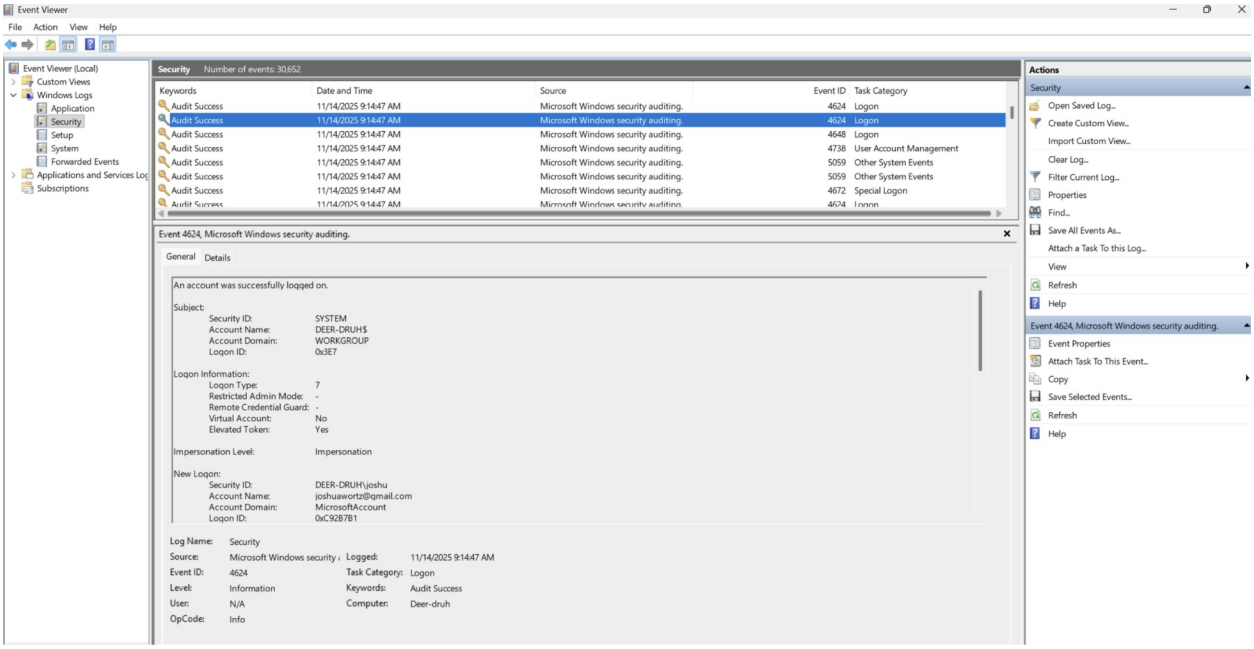
Summary:

A system-level logon event occurred (Logon Type 5), initiated by services.exe. The account authenticated successfully under the Negotiate package.

Interpretation:

Indicates expected system authentication behavior. Provides auditability and identity assurance required under SDL and OSA.

Screenshot:



Security Log – Event ID 4625 (Failed Logon)

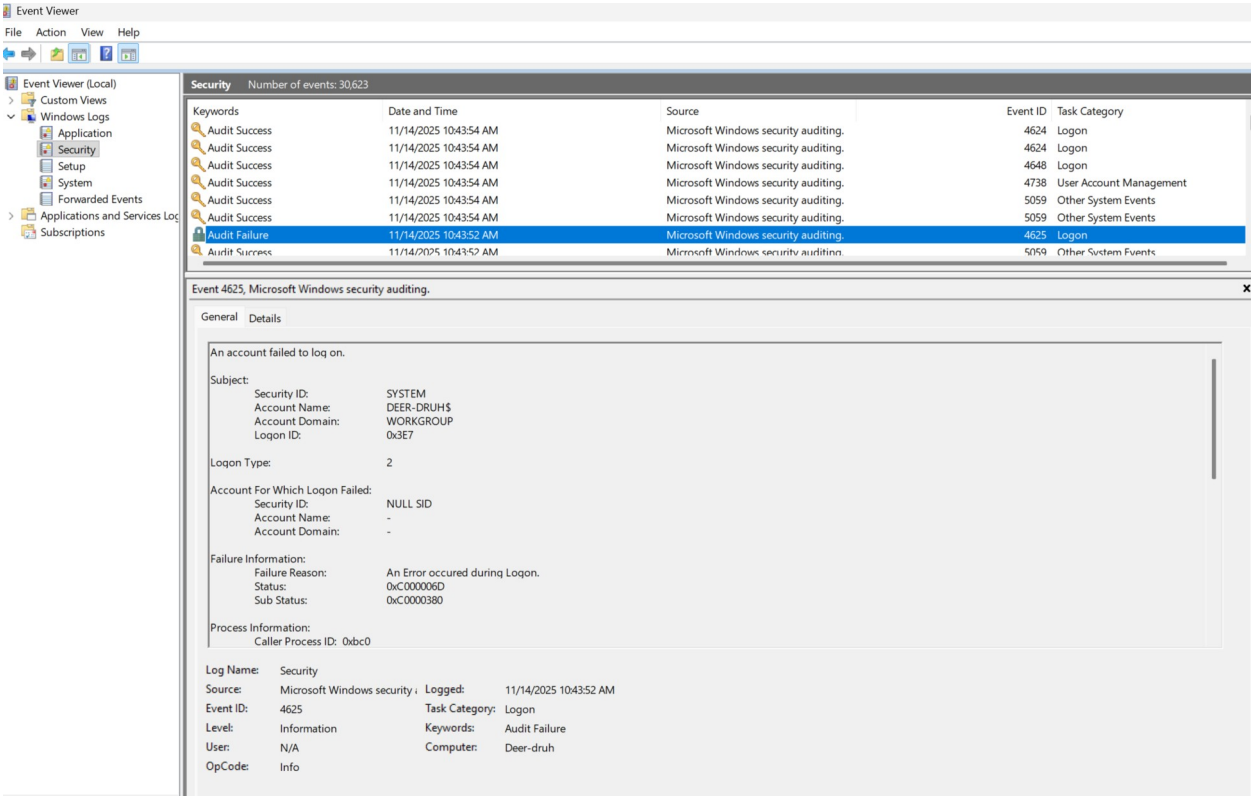
Summary:

A failed interactive logon occurred from 127.0.0.1 with error 0xC000006D. Originating process: svchost.exe.

Interpretation:

Failed authentication attempts provide critical anomaly detection. Repeated failures may indicate brute force attempts or misconfigurations.

Screenshot:



System Log – Event ID 7011 (WSLService Timeout)

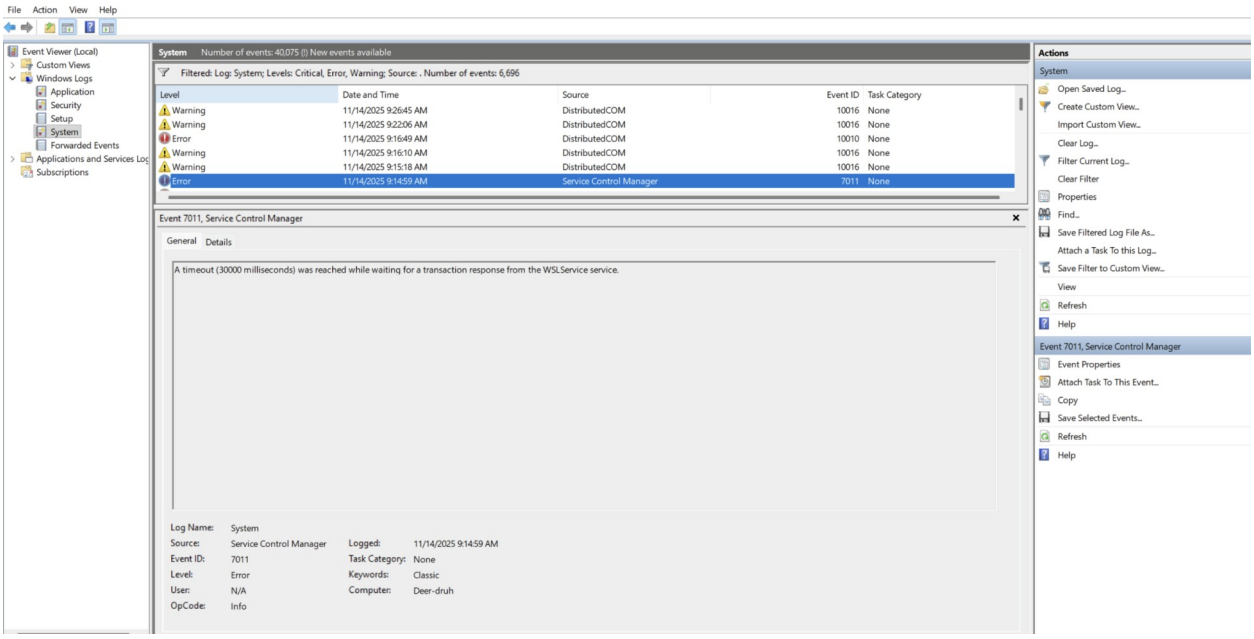
Summary:

Windows reported a timeout waiting for WSLService to respond within 30,000 ms.

Interpretation:

Service timeouts degrade reliability and can indicate system resource contention or configuration issues.

Screenshot:



Reliability Monitor – LightingService.exe Crash (BEX)

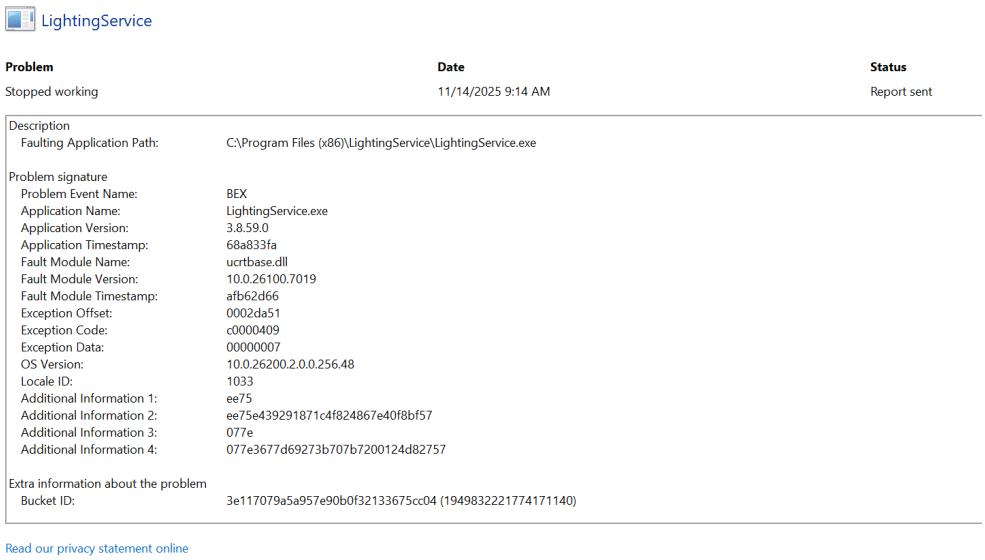
Summary:

LightingService crashed due to a Buffer Overflow Exception (BEX) in ucrtbase.dll.

Interpretation:

BEX exceptions can indicate memory corruption vulnerabilities. Third-party utilities often introduce risk due to insufficient hardening.

Screenshot:



LightingService

Problem	Date	Status
Stopped working	11/14/2025 9:14 AM	Report sent

Description
Faulting Application Path: C:\Program Files (x86)\LightingService\LightingService.exe

Problem signature
Problem Event Name: BEX
Application Name: LightingService.exe
Application Version: 3.8.59.0
Application Timestamp: 68a833fa
Fault Module Name: ucrtbase.dll
Fault Module Version: 10.0.26100.7019
Fault Module Timestamp: afb62d66
Exception Offset: 0002da51
Exception Code: c0000409
Exception Data: 00000007
OS Version: 10.0.26200.2.0.0.256.48
Locale ID: 1033
Additional Information 1: ee75
Additional Information 2: ee75e439291871c4f824867e40f8bf57
Additional Information 3: 077e
Additional Information 4: 077e3677d69273b707b7200124d82757

Extra information about the problem
Bucket ID: 3e117079a5a957e90b0f32133675cc04 (1949832221774171140)

Read our privacy statement online

Reliability Monitor – NvContainer.exe Crash (APPCRASH)

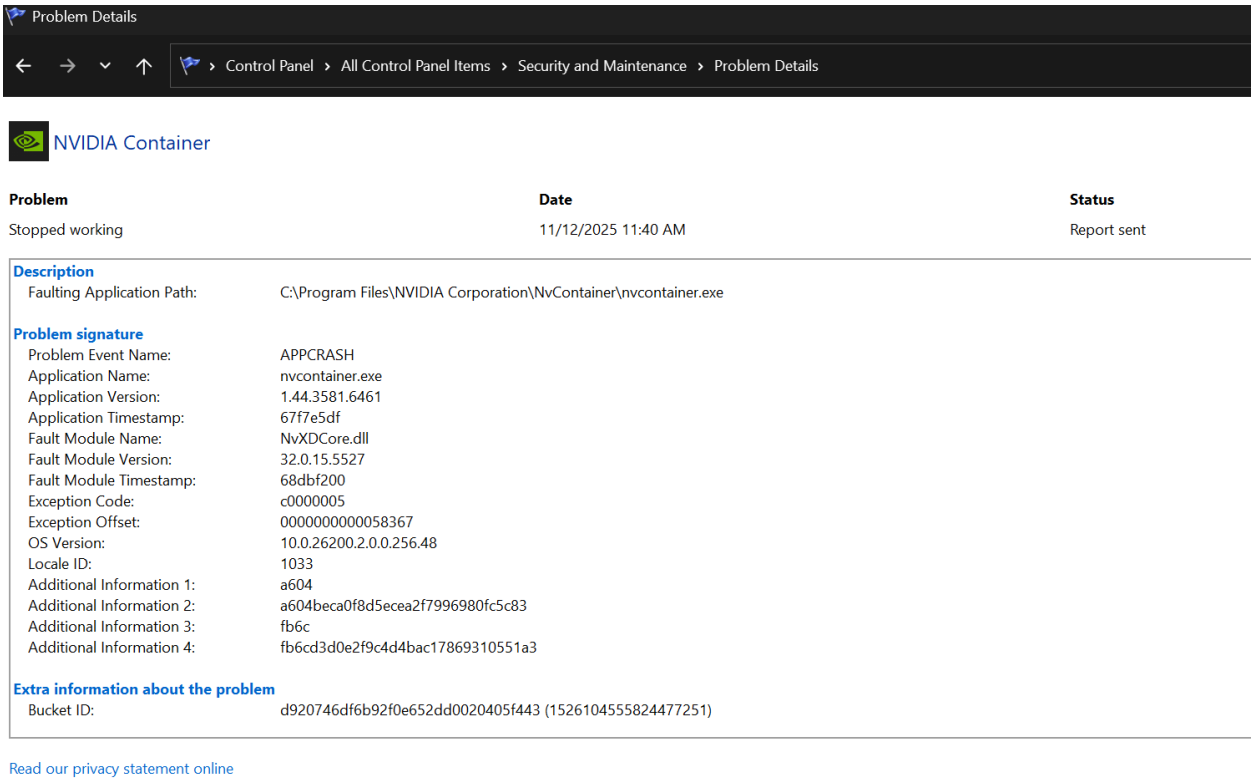
Summary:

NVIDIA's nvcontainer.exe crashed due to an exception in NvXDCore.dll.

Interpretation:

Driver instability is a known attack vector; unstable drivers can facilitate kernel-level compromise (Monzani et al., 2026).

Screenshot:



Framework Mapping

ISO 27001:2013 Alignment

Event	ISO 27001 Control
Logon auditing (4624/4625)	A.12.4.1: Event Logging
Failed authentication	A.12.4.3: Administrator and Operator Logs

WSLService timeout	A.12.1.3: Capacity Management
Application crashes	A.14.2.5: Secure System Engineering

NIST CSF Alignment

Event	NIST CSF Subcategory
Authentication events	PR.AC-7, DE.CM-7
Failed authentication	DE.AE-1, DE.AE-2
Service timeout	DE.CM-1
Driver/app crashes	RS.AN-1

Leadership Implications

Cybersecurity leaders rely on system telemetry to make informed decisions about system health, authentication patterns, service reliability, and third-party risk. The logs analyzed here highlight:

- Importance of monitoring authentication behavior
- Risk of unstable drivers and third-party tools
- Value of audit logs as a forensic and operational tool

- Importance of event baselines for anomaly detection

These insights support SDL's purpose: security must continue through operation, not end at deployment.

Conclusion

This Windows 11 environment demonstrates how Microsoft SDL and OSA influence secure system behavior. Authentication logs support auditability: service logs reveal reliability trends, application crashes highlight vulnerable components, and missing logs demonstrate the secure-by-default minimization of exposed attack surface. Mapped to ISO 27001 and NIST CSF, these findings demonstrate that even non-enterprise Windows environments offer robust foundational security. Together, these results reinforce the importance of SDL-aligned monitoring and secure operational practices in modern cyber defense.

References

Alharbi, S. J., & Moulahi, T. (2023). API security testing: The challenges of security testing for RESTful APIs. *International Journal of Innovative Science and Research Technology, 8*(5), 1485–1495. https://doi.org/10.5281/zenodo.7988410

Microsoft. (2023). *Security Development Lifecycle (SDL) practices.* Microsoft Technical Whitepaper.

Microsoft. (2024). *Operational Security Assurance for Microsoft 365.* Microsoft Technical Whitepaper.

Monzani, A., et al. (2026). Malware's use and abuse of kernel drivers. *NDSS Symposium 2026.*

Xiang, B., et al. (2025). Pig in a poke: Automatically detecting and exploiting link-following vulnerabilities in Windows. *USENIX Security Symposium 2025.* https://doi.org/10.5555/3766078.3766438

Yan, H., Chen, Y., Kang, Y., Guo, H., & Gu, X. (2024). LDR: Secure and efficient Linux driver runtime for ARM TrustZone. *NDSS Symposium 2024.* https://doi.org/10.14722/ndss.2024.23009

APPENDICES

Appendix A — Event ID 4624 (Successful Logon)

Log Name: *Security*

Source: *Microsoft-Windows-Security-Auditing*

Date: *11/14/2025 10:17:29 AM*

Event ID: *4624*

Task Category: Logon

Level: *Information*

Keywords: *Audit Success*

User: *N/A*

Computer: *Deer-druh*

Description:

An account was successfully logged on.

Subject:

Security ID: SYSTEM

Account Name: DEER-DRUH$

Account Domain: WORKGROUP

Logon ID: 0x3E7

Logon Information:

Logon Type: 7

Restricted Admin Mode: -

Remote Credential Guard: -

Virtual Account: No

Elevated Token: No

Impersonation Level: Impersonation

New Logon:

Security ID: DEER-DRUH\joshu

Account Name: joshuawortz@gmail.com

Account Domain: MicrosoftAccount

Logon ID: 0xE907215

Linked Logon ID: 0xE906FBB

Network Account Name: -

Network Account Domain: -

Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x7a8

Process Name: C:\Windows\System32\lsass.exe

Network Information:

Workstation Name: DEER-DRUH

Source Network Address: -

Source Port: -

Detailed Authentication Information:

Logon Process: Negotiat

Authentication Package: Negotiate

Transited Services: -

Package Name (NTLM only): -

Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The impersonation level field indicates the extent to which a process in the logon session can impersonate.

The authentication information fields provide detailed information about this specific logon request.

- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.

- Transited services indicate which intermediate services have participated in this logon request.

- Package name indicates which sub-protocol was used among the NTLM protocols.

- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Event Xml:

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

<System>

<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />

<EventID>4624</EventID>

<Version>3</Version>

<Level>0</Level>

<Task>12544</Task>

<Opcode>0</Opcode>

<Keywords>0x8020000000000000</Keywords>

<TimeCreated SystemTime="2025-11-14T18:17:29.9498270Z" />

<EventRecordID>2706467</EventRecordID>

<Correlation />

<Execution ProcessID="1960" ThreadID="15428" />

<Channel>Security</Channel>

<Computer>Deer-druh</Computer>

<Security />

</System>

<EventData>

<Data Name="SubjectUserSid">S-1-5-18</Data>

<Data Name="SubjectUserName">DEER-DRUH$</Data>

<Data Name="SubjectDomainName">WORKGROUP</Data>

<Data Name="SubjectLogonId">0x3e7</Data>

<Data Name="TargetUserSid">S-1-5-21-3599967172-1965848892-4195715880-1001</Data>

<Data Name="TargetUserName">joshuawortz@gmail.com</Data>

<Data Name="TargetDomainName">MicrosoftAccount</Data>

<Data Name="TargetLogonId">0xe907215</Data>

<Data Name="LogonType">7</Data>

<Data Name="LogonProcessName">Negotiat</Data>

<Data Name="AuthenticationPackageName">Negotiate</Data>

<Data Name="WorkstationName">DEER-DRUH</Data>

<Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>

<Data Name="TransmittedServices">-</Data>

<Data Name="LmPackageName">-</Data>

<Data Name="KeyLength">0</Data>

<Data Name="ProcessId">0x7a8</Data>

<Data Name="ProcessName">C:\Windows\System32\lsass.exe</Data>

<Data Name="IpAddress">-</Data>

<Data Name="IpPort">-</Data>

<Data Name="ImpersonationLevel">%%1833</Data>

<Data Name="RestrictedAdminMode">-</Data>

<Data Name="RemoteCredentialGuard">-</Data>

<Data Name="TargetOutboundUserName">-</Data>

<Data Name="TargetOutboundDomainName">-</Data>

<Data Name="VirtualAccount">%%1843</Data>

<Data Name="TargetLinkedLogonId">0xe906fbb</Data>

<Data Name="ElevatedToken">%%1843</Data>

</EventData>

</Event>

Appendix B — Event ID 4625 (Failed Logon)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Date: 11/14/2025 10:17:28 AM

Event ID: 4625

Task Category: Logon

Level: Information

Keywords: Audit Failure

User: N/A

Computer: Deer-druh

Description:

An account failed to log on.

Subject:

Security ID: SYSTEM

Account Name: DEER-DRUH$

Account Domain: WORKGROUP

Logon ID: 0x3E7

Logon Type: 2

Account For Which Logon Failed:

Security ID: NULL SID

Account Name: -

Account Domain: -

Failure Information:

Failure Reason: An Error occured during Logon.

Status: 0xC000006D

Sub Status: 0xC0000380

Process Information:

Caller Process ID: 0xbc0

Caller Process Name: C:\Windows\System32\svchost.exe

Network Information:

Workstation Name: -

Source Network Address: 127.0.0.1

Source Port: 0

Detailed Authentication Information:

Logon Process: User32

Authentication Package: Negotiate

Transited Services: -

Package Name (NTLM only): -

Key Length: 0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system requested the logon.

The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon request.

- Transited services indicate which intermediate services have participated in this logon request.

- Package name indicates which sub-protocol was used among the NTLM protocols.

- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Event Xml:

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

<System>

<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />

<EventID>4625</EventID>

<Version>0</Version>

<Level>0</Level>

<Task>12544</Task>

<Opcode>0</Opcode>

<Keywords>0x8010000000000000</Keywords>

<TimeCreated SystemTime="2025-11-14T18:17:28.0492051Z" />

<EventRecordID>2706454</EventRecordID>

<Correlation ActivityID="{0239c3f2-540d-000a-32e4-39020d54dc01}" />

<Execution ProcessID="1960" ThreadID="29752" />

<Channel>Security</Channel>

<Computer>Deer-druh</Computer>

<Security />

</System>

<EventData>

<Data Name="SubjectUserSid">S-1-5-18</Data>

<Data Name="SubjectUserName">DEER-DRUH$</Data>

<Data Name="SubjectDomainName">WORKGROUP</Data>

<Data Name="SubjectLogonId">0x3e7</Data>

<Data Name="TargetUserSid">S-1-0-0</Data>

<Data Name="TargetUserName">-</Data>

<Data Name="TargetDomainName">-</Data>

<Data Name="Status">0xc000006d</Data>

<Data Name="FailureReason">%%2304</Data>

<Data Name="SubStatus">0xc0000380</Data>

<Data Name="LogonType">2</Data>

<Data Name="LogonProcessName">User32 </Data>

<Data Name="AuthenticationPackageName">Negotiate</Data>

<Data Name="WorkstationName">-</Data>

<Data Name="TransmittedServices">-</Data>

<Data Name="LmPackageName">-</Data>

<Data Name="KeyLength">0</Data>

<Data Name="ProcessId">0xbc0</Data>

<Data Name="ProcessName">C:\Windows\System32\svchost.exe</Data>

<Data Name="IpAddress">127.0.0.1</Data>

<Data Name="IpPort">0</Data>

</EventData>

</Event>

Appendix C — System Log Event ID 7011 (WSLService Timeout)

Log Name: System

Source: Service Control Manager

Date: 11/14/2025 9:14:59 AM

Event ID: 7011

Task Category: None

Level: Error

Keywords: Classic

User: N/A

Computer: Deer-druh

Description:

A timeout (30000 milliseconds) was reached while waiting for a transaction response from the WSLService service.

Event Xml:

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

<System>

<Provider Name="Service Control Manager" Guid="{555908d1-a6d7-4695-8e1e-26931d2012f4}" EventSourceName="Service Control Manager" />

<EventID Qualifiers="49152">7011</EventID>

```
  <Version>0</Version>
  <Level>2</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8080000000000000</Keywords>
  <TimeCreated SystemTime="2025-11-14T17:14:59.2635640Z" />
  <EventRecordID>193747</EventRecordID>
  <Correlation />
  <Execution ProcessID="1932" ThreadID="55476" />
  <Channel>System</Channel>
  <Computer>Deer-druh</Computer>
  <Security />
</System>
<EventData>
  <Data Name="param1">30000</Data>
  <Data Name="param2">WSLService</Data>
</EventData>
```

</Event>

Appendix D — LightingService.exe Crash (BEX)

Source

LightingService

Summary

Stopped working

Date

11/14/2025 9:14 AM

Status

Report sent

Description

Faulting Application Path: C:\Program Files (x86)\LightingService\LightingService.exe

Problem signature

Problem Event Name: BEX

Application Name: LightingService.exe

Application Version: 3.8.59.0

Application Timestamp: 68a833fa

Fault Module Name: ucrtbase.dll

Fault Module Version: 10.0.26100.7019

Fault Module Timestamp: afb62d66

Exception Offset: 0002da51

Exception Code: c0000409

Exception Data: 00000007

OS Version: 10.0.26200.2.0.0.256.48

Locale ID: 1033

Additional Information 1: ee75

Additional Information 2: ee75e439291871c4f824867e40f8bf57

Additional Information 3: 077e

Additional Information 4: 077e3677d69273b707b7200124d82757

Extra information about the problem

Bucket ID: 3e117079a5a957e90b0f32133675cc04 (1949832221774171140)

Appendix E — nvcontainer.exe Crash (APPCRASH)

Source

NVIDIA Container

Summary

Stopped working

Date

11/12/2025 11:40 AM

Status

Report sent

Description

Faulting Application Path: C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe

Problem signature

Problem Event Name: APPCRASH

Application Name: nvcontainer.exe

Application Version: 1.44.3581.6461

Application Timestamp: 67f7e5df

Fault Module Name: NvXDCore.dll

Fault Module Version: 32.0.15.5527

Fault Module Timestamp: 68dbf200

Exception Code: c0000005

Exception Offset: 0000000000058367

OS Version: 10.0.26200.2.0.0.256.48

Locale ID: 1033

Additional Information 1: a604

Additional Information 2: a604beca0f8d5ecea2f7996980fc5c83

Additional Information 3: fb6c

Additional Information 4: fb6cd3d0e2f9c4d4bac17869310551a3

Extra information about the problem

Bucket ID: d920746df6b92f0e652dd0020405f443 (1526104555824477251)