## Case report for event ID: 1001

| ID | Alert rule | Description | Incident type | Severity level | Date and time detected |
|---|---|---|---|---|---|
| 1001 | Suspicious Parent Child Relationship | A suspicious process with an uncommon parent-child relationship was detected in your environment. | Process | Low | Nov 28th 2025 at 19:31 |

Alert details

datasource: sysmon

timestamp: 11/28/2025 11:29:21.272

event.code: 1

host.name: win-3459

process.name: TrustedInstaller.exe

process.pid: 3577

process.parent.pid: 3506

process.parent.name: services.exe

process.command_line: C:\Windows\servicing\TrustedInstaller.exe

process.working_directory: C:\Windows\system32\

event.action: Process Create (rule: ProcessCreate)

## Incident report

Edit report

**Incident classification**

○ True positive ◉ False positive

**Closure rationale**

Explain why you have identified this incident as a false positive.

**Time of Activity:** 11/28/2025 11:29:21.272
**Data Source:** Sysmon (Event ID 1 – Process Create)
**List of Related Entities:**
- **Host:** win-3459
- **Process:** TrustedInstaller.exe (PID 3577)
- **Parent Process:** services.exe (PID 3506)

**Description of Activity:** Sysmon detected the creation of `TrustedInstaller.exe` with parent process `services.exe`. While the detection rule flagged this as an uncommon parent-child relationship, this behavior is consistent with legitimate Windows servicing operations.
**Reason for Classifying as False Positive:**
- `TrustedInstaller.exe` is a legitimate Windows process responsible for installing, modifying, and removing system updates and components.
- Its execution from `C:\Windows\servicing\TrustedInstaller.exe` with parent `services.exe` aligns with expected behavior during system maintenance.
- No anomalous command-line arguments or suspicious working directory were observed.

**Reason for Not Escalating the Alert:**
- The activity matches normal Windows servicing operations.
- No indicators of compromise (IoCs) or malicious intent were identified.
- Escalation is unnecessary; instead, detection rule tuning should be applied to reduce noise.

**Recommended Remediation Actions:**

Save and close alert

**Complete IR:**

Time of Activity: 11/28/2025 11:29:21.272

Data Source: Sysmon (Event ID 1 – Process Create)

List of Related Entities:

Host: win-3459

Process: TrustedInstaller.exe (PID 3577)

Parent Process: services.exe (PID 3506)

Description of Activity: Sysmon detected the creation of TrustedInstaller.exe with parent process services.exe. While the detection rule flagged this as an uncommon parent-child relationship, this behavior is consistent with legitimate Windows servicing operations.

Reason for Classifying as False Positive:

TrustedInstaller.exe is a legitimate Windows process responsible for installing, modifying, and removing system updates and components.

Its execution from C:\Windows\servicing\TrustedInstaller.exe with parent services.exe aligns with expected behavior during system maintenance.

No anomalous command-line arguments or suspicious working directory were observed.

Reason for Not Escalating the Alert:

The activity matches normal Windows servicing operations.

No indicators of compromise (IoCs) or malicious intent were identified.

Escalation is unnecessary; instead, detection rule tuning should be applied to reduce noise.

Recommended Remediation Actions:

Fine-tune detection rules to whitelist TrustedInstaller.exe when spawned by services.exe.

Continue monitoring for deviations (e.g., unexpected parent processes or unusual command-line arguments).

Document this case as a known benign pattern to improve SOC efficiency.

List of Attack Indicators (None observed):

No suspicious command-line arguments.

No abnormal working directory.

No unusual parent process beyond expected services.exe.