Vulnerabilities in Microsoft SQL Server Reporting Services and Windows Task Scheduler – CVE-2020-0618 and CVE-2019-1069

Overview

Two Microsoft vulnerabilities have been reported and added to the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalog this week.

CVE-2020-0618 (CVSS 8.8)

A vulnerability (CVE-2020-0618) has been found in Microsoft SQL Server Reporting Services. This vulnerability stems from a deserialization flaw, allowing authenticated attackers to execute arbitrary code with the same privileges as the Report Server service account. The flaw occurs when the service improperly handles page requests, leading to potential remote code execution. Exploiting this vulnerability could compromise the server's data and overall functionality.

This vulnerability requires authenticated access to the SQL Server Reporting Services, meaning the attacker needs valid credentials before exploitation. While it involves a deserialization flaw (a relatively common weakness), obtaining valid credentials might be a barrier. However, once authenticated, the deserialization flaw can be exploited relatively easily

CVE-2019-1069 (CVSS 7.8)

CVE-2019-1069 addresses a privilege escalation flaw in Microsoft Windows Task Scheduler. This vulnerability is linked to the **SetJobFileSecurityByName()** function, which allows a local authenticated attacker to gain SYSTEM-level privileges. With this elevated access, the attacker could take full control of the affected system.

To exploit this vulnerability, the attacker needs local access to the system, either physically or through remote access with valid credentials. Privilege escalation vulnerabilities are typically easier to exploit once the attacker has local access.

Although CVE-2020-0618 and CVE-2019-1069 are older vulnerabilities, they have been actively exploited in the wild. Aspire strongly advises users to apply the necessary patches and mitigations to help prevent attacks.

Aspire Protects

- CVE-2020-0618
    - Organizations using Microsoft SQL Server Reporting Services are urged to promptly apply the patches issued by Microsoft.
    - The patch addresses the vulnerability by modifying how the Microsoft SQL Server Reporting Services handles page requests. Please see Microsoft's advisory for patch guidance.
- CVE-2019-1069
    - Organizations should prioritize applying the recommended patches from Microsoft to secure systems.
    - The patch addresses the vulnerability by correctly validating file operations. Please see Microsoft's advisory for patch guidance.
- For any questions, please reach out to Aspire's Customer Success Management team.

IoCs

There are no known IoCs for CVE-2020-0618 and CVE-2019-1069 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

TTPs to Watch

CVE-2020-0618

- **Tactic: Initial Access (TA0001)**
    - Valid Accounts (T1078) - Attackers leverage valid credentials to authenticate and access the vulnerable SQL Server Reporting Services.
- **Tactic: Execution (TA0002)**
    - Exploitation for Client Execution (T1203) - Attackers exploit the deserialization vulnerability in the SQL Server to execute arbitrary code on the system.
    - Command and Scripting Interpreter (T1059) - The arbitrary code execution often involves scripts or commands on the server for further malicious activity.
- **Tactic: Execution (TA0002)**
    - Exploitation for Client Execution (T1203) - Attackers exploit the deserialization vulnerability in the SQL Server to execute arbitrary code on the system.
    - Command and Scripting Interpreter (T1059) - The arbitrary code execution often involves scripts or commands on the server for further malicious activity.
- **Tactic: Defense Evasion (TA0005)**
    - Masquerading (T1036) - Malicious code may be disguised to look like legitimate Report Server activity.

CVE-2019-1069

- **Tactic: Privilege Escalation (TA0004)**
  - Exploitation for Privilege Escalation (T1068) - Attackers exploit the vulnerability in the Task Scheduler to gain SYSTEM-level privileges on the host system.
- **Tactic: Execution (TA0002)**
  - Scheduled Task/Job (T1053**)** - Attackers use the Task Scheduler to execute commands or malware with elevated SYSTEM privileges.
  - Command and Scripting Interpreter (T1059) - Post-exploitation, attackers may execute additional commands or scripts using the elevated privileges obtained from the Task Scheduler.
- **Tactic: Persistence (TA0003)**
  - Boot or Logon Autostart Execution (T1547) - Attackers could create or modify system files to enable malware persistence during system reboots.
- **Tactic: Defense Evasion (TA0005)**
  - Process Injection (T1055) - Attackers may inject malicious code into legitimate processes to evade detection and maintain persistence.
  - Masquerading (T1036) - The use of legitimate system tools like Task Scheduler can help attackers avoid detection by blending in with normal system operations.
- **Tactic: Impact (TA0040)**
  - Inhibit System Recovery (T1490) - Attackers may disable system recovery features such as backups or restoration points to ensure their activities go unnoticed and are hard to recover from.

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

Supporting Documentation

CVE-2020-0618 - Security Update Guide - Microsoft - Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability

CVE-2019-1069 - Security Update Guide - Microsoft - Task Scheduler Elevation of Privilege Vulnerability

NVD - CVE-2019-1069 (nist.gov)

NVD - cve-2020-0618 (nist.gov)