Smarttech

YOUR 24/7 SECURITY PARTNER

Threat Report

Microsoft Patch Tuesday – April 2024

NSAI

QUALITY
I.S. EN ISO 27001:2013
NSAI Certified

QUALITY
I.S. EN ISO 9001:2015
NSAI Certified

Document ID	SMA- Threat Report
Document status	ISSUED
Issue Number	02
Authors	Razvan Constantin < razvan.constantin@smarttech247.com >
Verified by	Alin Curcan <alin.curcan@smarttech247.com>
Last modified	2024-04-10
Issue Date	2024-04-09

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.

Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Microsoft's April 2024 Patch Tuesday addressed 149 vulnerabilities, including sixty-seven remote code execution flaws. Among these, only three critical vulnerabilities are addressed, successful exploitation of these vulnerabilities could allow remote code execution and elevation of privilege.

The breakdown of vulnerabilities includes:

- 67 Remote Code Execution Vulnerabilities
- 31 Elevation of Privilege Vulnerabilities
- 27 Security Feature Bypass Vulnerabilities
- 12 Information Disclosure Vulnerabilities
- 7 Denial of Service Vulnerabilities
- 3 Spoofing Vulnerabilities

RISK

Government:

- Large and medium government entities: **HIGH**
- Small government entities: **MEDIUM**

Businesses:

- Large and medium business entities: **HIGH**
- Small business entities: **MEDIUM**

Flaws of interest

This month's Patch Tuesday doesn't address any zero-day vulnerabilities but does include some noteworthy flaws:

1. CVE-2024-29988 - SmartScreen Prompt Security Feature Bypass Vulnerability - is a security feature bypass vulnerability in Microsoft Defender SmartScreen. It was assigned a CVSSv3 score of 8.8 and is rated as important. An attacker could exploit this vulnerability by convincing a target to open a specially crafted file using social engineering tactics such as an external link or malicious attachment sent over email, instant messages or social media.This flaw was reported to Microsoft by some of the same researchers that disclosed CVE-2024-21412, an Internet Shortcut Files security feature bypass that was associated with a DarkGate campaign using fake installer files impersonating Apple iTunes, Notion, NVIDIA and others.

2. CVE-2024-29988 - SmartScreen Prompt Security Feature Bypass Vulnerability - is a security feature bypass vulnerability in Microsoft Defender SmartScreen. It was assigned a CVSSv3 score of 8.8 and is rated as important. An attacker could exploit this vulnerability by convincing a target to open a specially crafted file using social engineering tactics such as an external link or malicious attachment sent over email, instant messages or social media.This flaw was reported to Microsoft by some of the same researchers that disclosed CVE-2024-21412, an Internet Shortcut Files security feature bypass that was associated with a DarkGate campaign using fake installer files impersonating Apple iTunes, Notion, NVIDIA and others.

3. CVE-2024-29990 | Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability - is an EoP vulnerability in the Azure Kubernetes Service Confidential Containers (AKSCC). It was assigned a CVSSv3 score of 9 and is rated important. Exploitation of this flaw hinges on the preparation of a target environment by an attacker. Successful exploitation would enable an attacker to “steal credentials and affect resources beyond the security scope managed by AKSCC.” This includes taking over both “confidential guests and containers beyond the network stack it might be bound to.”

SYSTEMS AFFECTED:

Description	CVE ID	CVSS Score	Severity
Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	CVE-2024-21400	9	Critical
Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	CVE-2024-21403	9	Critical
	CVE-2024-21376	9	Critical
Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	CVE-2024-28929	8.8	High
	CVE-2024-28930	8.8	High
	CVE-2024-28931	8.8	High
	CVE-2024-28932	8.8	High
	CVE-2024-28933	8.8	High
	CVE-2024-28934	8.8	High
	CVE-2024-28935	8.8	High
	CVE-2024-28936	8.8	High
	CVE-2024-28937	8.8	High
	CVE-2024-28938	8.8	High
	CVE-2024-28941	8.8	High
	CVE-2024-28943	8.8	High
	CVE-2024-29043	8.8	High
Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	CVE-2024-28906	8.8	High
	CVE-2024-28908	8.8	High
	CVE-2024-28909	8.8	High
	CVE-2024-28910	8.8	High
	CVE-2024-28911	8.8	High
	CVE-2024-28912	8.8	High
	CVE-2024-28913	8.8	High
	CVE-2024-28914	8.8	High
	CVE-2024-28915	8.8	High

	CVE-2024-28926	8.8	High
	CVE-2024-28927	8.8	High
	CVE-2024-28939	8.8	High
	CVE-2024-28940	8.8	High
	CVE-2024-28942	8.8	High
	CVE-2024-28944	8.8	High
	CVE-2024-28945	8.8	High
	CVE-2024-29044	8.8	High
	CVE-2024-29045	7.5	High
	CVE-2024-29047	8.8	High
	CVE-2024-29048	8.8	High
	CVE-2024-29982	8.8	High
	CVE-2024-29983	8.8	High
	CVE-2024-29984	8.8	High
	CVE-2024-29985	8.8	High
	CVE-2024-29046	8.8	High
Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability	CVE-2024-26210	8.8	High
	CVE-2024-26244	8.8	High
Microsoft WDAC SQL Server ODBC Driver Remote Code Execution Vulnerability	CVE-2024-26214	8.8	High
Secure Boot Security Feature Bypass Vulnerability	CVE-2024-26240	8	High
	CVE-2024-26189	8	High
	CVE-2024-28925	8	High
	CVE-2024-26180	8	High
	CVE-2024-29061	7.8	High
	CVE-2024-28920	7.8	High
	CVE-2024-26175	7.8	High
	CVE-2024-28896	7.5	High
	CVE-2024-26194	7.4	High
	CVE-2024-20688	7.1	High
	CVE-2024-29062	7.1	High
	CVE-2024-20689	7.1	High
	CVE-2024-28897	6.8	Medium
	CVE-2024-26168	6.8	Medium
	CVE-2024-28919	6.7	Medium
	CVE-2024-26250	6.7	Medium
	CVE-2024-20669	6.7	Medium
	CVE-2024-28924	6.7	Medium
	CVE-2024-26171	6.7	Medium
	CVE-2024-28921	6.7	Medium
	CVE-2024-28923	6.4	Medium
	CVE-2024-28898	6.3	Medium
	CVE-2024-28922	4.1	Medium

Recommendations

We recommend the following actions be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Apply the Principle of Least Privilege to all systems and services, and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
  - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
  - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (**M1017: User Training**)
  - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
  - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
  - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

Reference:

- https://www.tenable.com/blog/microsofts-april-2024-patch-tuesday-addresses-147-cves-cve-2024-29988
- April 2024 Security Updates - Release Notes - Security Update Guide - Microsoft