Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's February 2024 Patch Tuesday Addresses Three Zero-day Vulnerabilities

Date of Publication	Last updated date	Admiralty Code	TA Number
February 14, 2024	February 23, 2024	A1	TA2024057

Summary

First Seen: February 13, 2024
Affected Platforms: Microsoft Windows SmartScreen, Internet Shortcut Files, Windows Win32k, Windows Kernel, Windows Pragmatic General Multicast (PGM), Microsoft Outlook, Microsoft Word, Microsoft Exchange Server and more
Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Information Disclosure, Remote Code Execution (RCE), Security Feature Bypass, and Spoofing

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-21351	Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows SmartScreen	✓	✓	✓
CVE-2024-21412	Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Internet Shortcut Files	✓	✓	✓
CVE-2024-21410	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✓	✓	✓
CVE-2024-21413	Microsoft Outlook Remote Code Execution Vulnerability	Microsoft Outlook	✗	✗	✓
CVE-2024-21338	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows Kernel	✗	✗	✓
CVE-2024-21357	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	Microsoft Windows Pragmatic General Multicast (PGM)	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-21371	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows Kernel	✗	✗	✓
CVE-2024-21378	Microsoft Outlook Remote Code Execution Vulnerability	Microsoft Outlook	✗	✗	✓
CVE-2024-21379	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	✗	✗	✓
CVE-2024-21346	Win32k Elevation of Privilege Vulnerability	Microsoft Windows Win32k	✗	✗	✓
CVE-2024-21345	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows Kernel	✗	✗	✓

Vulnerability Details

#1

Microsoft's February 2024 Patch Tuesday includes security updates for a total of 73 vulnerabilities, comprising five critical, 66 important, and two moderate vulnerabilities. The breakdown of vulnerabilities includes 16 Elevation of Privilege, 30 Remote Code Execution, 5 Information Disclosure, 3 Security Feature Bypass, 9 Denial of Service, and 10 Spoofing vulnerabilities.

#2

The updates cover various Microsoft products such as Office, SQL Server, .NET, Azure, Windows, Defender for Endpoint, Windows SmartScreen, Windows Win32K, Windows Kernel, Windows Hyper-V, Windows Internet Connection Sharing (ICS) and more. Notably, Microsoft patched six vulnerabilities in the Chromium-based Microsoft Edge browser, bringing the total number of CVEs to 79. Among these, two vulnerabilities have been actively exploited in the wild. This advisory pertains to 11 CVEs that could potentially be exploited.

#3 One of the critical patches, CVE-2024-21351, involves a Windows SmartScreen Security Feature Bypass, allowing attackers to bypass SmartScreen security checks. Microsoft highlights that an attacker needs to send a malicious file to the user and convince them to open it, thereby bypassing the SmartScreen user experience. The specific exploitation methods or threat actors behind these attacks remain undisclosed at this time. It has been exploited in the wild as a zero-day. Notably, this marks the fifth SmartScreen vulnerability disclosed since 2022, all (CVE-2022-44698, CVE-2023-24880, CVE-2023-32049, CVE-2023-36025) have been exploited as zero-days.

#4 The second zero-day vulnerability, CVE-2024-21412, concerns an Internet Shortcut Files Security Feature Bypass, which could circumvent Mark of the Web (MoTW) warnings in Windows. An unauthenticated attacker could send a specially crafted file to the targeted user, attempting to bypass displayed security checks. The attacker's ability to coerce users into clicking the file link is crucial for exploitation.

#5 CVE-2024-21410 is another zero-day critical elevation of privilege (EoP) vulnerability in Microsoft Exchange Server, with a CVSS score of 9.8. It enables attackers to leak NTLM credentials from an NTLM client like Outlook, then utilize them to gain privileges on the Exchange server and perform actions as the victim client.

#6 CVE-2024-21413, also known as the MonikerLink bug, is another critical vulnerability in Microsoft Outlook. It allows attackers to bypass Protected View, granting high privileges and potentially leading to the leakage of local NTLM credentials and remote code execution (RCE).

#7 Additional notable vulnerabilities include CVE-2024-21378, an RCE flaw in Microsoft Outlook, CVE-2024-21346, an EoP vulnerability in Win32k, CVE-2024-21379, an RCE issue in Microsoft Word, CVE-2024-21345, CVE-2024-21371, and CVE-2024-21338, all EoP vulnerabilities in Windows Kernel. These vulnerabilities highlight the diverse range of threats addressed in this update.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21351	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-254

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21412	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-254
CVE-2024-21410	Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018	cpe:2.3:a:microsoft:exchange_server:2016:cu23:*:*:*:*:*:*:*	CWE-668
CVE-2024-21413	Microsoft Office: 2016 - 2019 Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-21338	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-264
CVE-2024-21357	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-21371	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-362
CVE-2024-21378	Microsoft Outlook: 2016 - 2019 Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:outlook:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	CWE-20

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21379	Microsoft Office: 2019 Microsoft Word: 2016 Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:word:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-21346	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-254
CVE-2024-21345	Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-264

Recommendations

- Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting security measures.
- Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.
- Prioritize critical vulnerabilities, especially CVE-2024-21351 (Windows SmartScreen Security Feature Bypass) and CVE-2024-21412 (Internet Shortcut Files Security Feature Bypass). These vulnerabilities have the potential for severe exploitation and should be addressed urgently.
- Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.
- Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0042 Resource Development	TA0007 Discovery	TA0002 Execution
TA0003 Persistence	TA0005 Defense Evasion	T1588 Obtain Capabilities	T1588.005 Exploits
T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1203 Exploitation for Client Execution
T1082 System Information Discovery	T1553.005 Mark-of-the-Web Bypass	T1553 Subvert Trust Controls	T1498 Network Denial of Service

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1458a762332676f7807ab45f8f236c22a1a7bb0c21fcd8c779f972f2446a11d0, 758c6364ab560fbeff2bfa8712a2e09132d85d0bf6918e6acc79fe12f5b71ec3, 77d685e29c3dbe75fa8a82c69c68c731a09904020a76145ca27aeaf0058455cd, b36dc329a5dc766c2645d5f5b6cdaa9542ec3b0aa1bc13dc1f899ce6d95d59fb, d895fff3c909ea2eb6624fc5f154c924fe0af51c6c899fd9093dc3cd27a5dad2, 008e57d62caa8cfa991f5519eabe3f15d79799b81ba8cc6b67cde6da0dbffdab, 087878208755420d5d7ae2eb6a84482768cb8972732911ac16096cd0c95fa0f7, 1115e4bed3949493d8ab184e5c42f047355f13b9bf91c1621acb7971a148bea2, 18b1dc2e00245cb017ebdedfe63881929d7542eeffa8f42ee0ad20cc2ebf181a, 1956bcd3df47e76b2e9f396514f072311563d092ae02509f817c488567749998, 1fbc621a71578cb22d4e3a0feec68735321358a3aeb18adbe4a20630c7f788b8, 39fb9fb06910f1133f3b23c523a5139f61d243380802b0670a664473d00e1fa9, 3e420ce1dc1a8503f48815b880381dd23206e08be2474d151f1353df7df2d796,

TYPE	VALUE
SHA256	4201ab8c0c4cf0f01f5a25d8e4e7221634776b5bad8c3faad5ad819ec58619ad, 58b0f5da4a53e956b35e77f55ced641291a596e16067b1dab6ac54d9cb6a52a5, 5b16ac1edb747053ee5a085ab826c61218c5b471eaa04f2471dc2e80b5621023, 5c85a0fe230d351b35da364c797cc95557f5dcceec034eb648e1805237c7203b, 5f4ef55201080ef3a62b0fbdc4c27e0ccdf4041f41c04471f35b127ff6515405, 61de01bc154b1118caacfed3839c996a795d6c21c2efbf1da6b926414f5d182d, 65cc5594b307c2ac4e3c251aeae68dedf7d1f24ba3b0d7ab5ad3623e8a9fc865, 6793e0fbc2def9173bf8e2a6c1aa357ba7fc3e32dc1cf81107677166f175c890, 6bec457f83d0d98f6f6ea1243c2327e012db38fb61680f6bd68dbab0dc07170a, 7058ae0f02e116b38536ee1ec20f47645aecf761361b5a5e85de2961f3cc88c6, 70b4c2d696a24a5ae2f5e5095dc44e68b4605e4690c8a49930194ee87eb80252, 73922ab0d048b45a01f13ba967f1423bc6cd6cc711f8e7d00a4cf2b1d3646f4e, 761fa42bc4cc5332a640c7389240324242981176ca1626e4267cc8a00cf9545f, 88bb1df99e02021801b08beeff87ec3ceb9e16c42f62904c5ac04c1a26213a48, 941cf63028bf8314bc7114a088f4d1f1dd995bec4a4b7c51fda34fbb3528667f, a45e0ea5a17ba6f3a2ce7258f6cc81c6f93f37873b49218a25ec638987da6f96, a5096c4624a523a660242e3451c2f4d644431a35098e36b724fab9f7d88d145d, a9633da58719f07159702101474b6ba78f2ffee28b3f7ebda3feb36db4e2d0e9, b0ab19986ab1297870854980f1287f1a4b8d003c540773a6c04fb3565e5701ee, b350a787c19a756c0824e14eec7e9d746450d1aafb28a5d15209ec9f34c58129, b738e92afc95cba819aa7aebfad459de38743c478e9e8b8f29f9919697b495b0, b8b6b6d98b7ea689f0c33d55a06afcf20482b25c51929ca9a1b302374290b337, babbd9c94dedb94be8baac2ddc5b4714c44a8d0c60d49c0dc91708784bc0d57f, bbdf52481bd1a15710d75b89240c7a360450e2f4f00ba2cb140affba79ebec94,

TYPE	VALUE
SHA256	c86ba0da732e1fa1f06549d3ebc5ae6ae091199e95930681ac2a9152a8834184, d6000a19198b8b9719fc17f7c06366e542802a8e7e232ba731b72c31226cc890, d81e7d95004441ea4f5344215232db57f48579bf335c7ba4ed7f6ec6f9136ed0, db1bc70c0d0c7121f1d4422a6fcd0e0668d9da786affb52dd77852641e425710, ddda5737b2c3207d72d728bf40709a7296c31e7c50951dcad441f4707581ccb1, e1b903eba88b920909876442306e1160eed9b69c69a05ea370cba2121e305ba1, e49a7d9083b2e448274d117405c39b0c1b2c0c20ab5195bdf94aaeda7cc113d7, f44964c8fdf6dbdb21c141df61b45467bba5a4482f7ab19fd6f1841fdb791f2a, f6b01df60d526f1de530230724d41b482adfff81084a1872bb97c316b76e45e3, f701f500d348b63f3250239cd8305a8b38230e67d74456f3333c6efeeef85bbb, fb67be10a5a8b26ca86f8f79935ddd4a5b40379bb6d0af21d23f56af14bb2a90, 4307a067db6b6abd852441e6d70de29c3bd0e4d6a68f0449b4034015187b7e037, 69fc5bed55acf559035f2c5550bf8807236b580f8e2db88966b3fc80c83914d3, 4c43b4575063d50ca5668e45a434aaf288970c89e8a4414812560ee787307f58, 135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c, 252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146, 594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978, 6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49, 71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc, b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a351d40422feb, bf9c3218f5929dfeccbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c, dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f3f5ecf54,

TYPE	VALUE
File Paths	/fxbulls, /fxbulls/pictures, /fxbulls/pictures/photo_2023-12-29[.]jpg[.]url, /fxbulls/pictures/Thumbs[.]db , /fxbulls/pictures/2[.]url , /fxbulls/pictures/a2[.]zip , /fxbulls/pictures/a2[.]zip/a2[.]cmd, /fxbulls/pictures/a2[.]zip, /fxbulls/pictures/b3[.]dll, /fxbulls/pictures/7z[.]dll, /fxbulls/pictures/7z[.]exe, /fxbulls/pictures/photo_2023-12-29s[.]jpg, /fxbulls/pictures/My2[.]zip, /fxbulls, /fxbulls/images, /fxbulls/images/photo_2023-12-29[.]jpg[.]url, /fxbulls/images/Thumbs[.]db , /fxbulls/images/2[.]url , /fxbulls/images/a2[.]zip , /fxbulls/images/a2[.]zip/a2[.]cmd, /fxbulls/images/a2[.]zip, /fxbulls/images/b3[.]dll, /fxbulls/images/7z[.]dll, /fxbulls/images/7z[.]exe, /fxbulls/images/photo_2023-12-29s[.]jpg, /fxbulls/images/My2[.]zip, /fxbulls/net, /fxbulls/net/photo_2023-12-29[.]jpg[.]url, /fxbulls/net/Thumbs[.]db , /fxbulls/net/2[.]url , /fxbulls/net/a2[.]zip , /fxbulls/net/a2[.]zip/a2[.]cmd, /fxbulls/net/a2[.]zip, /fxbulls/net/b3[.]dll, /fxbulls/net/7z[.]dll, /fxbulls/net/7z[.]exe, /fxbulls/net/photo_2023-12-29s[.]jpg, /fxbulls/net/My2[.]zip, /underwall/docs, /underwall/docs/7z.zip, /underwall/docs/passport.jpg.url, /underwall/docs/warop.url, /underwall/expand, /underwall/expand/7z.zip, /underwall/expand/photo_2023-12-26.jpg.url, /underwall/expand/warop.url, /underwall/society, /underwall/society/7z.zip, /underwall/society/photo_2023-12-26.jpg.url, /underwall/society/warop.url

TYPE	VALUE
Domains	fxbulls[.]ru, 87iavv[.]com, unfawjelesst322[.]com, p2oaviwt39ui[.]com
IPv4	84[.]32[.]189[.]74, 179[.]43[.]172[.]127, 179[.]43[.]172[.]191, 64[.]31[.]63[.]70, 64[.]31[.]63[.]194
URLs	hxxp[://]84[.]32[.]189[.]74, hxxp[://]84[.]32[.]189[.]74/xampp/, hxxp[://]84[.]32[.]189[.]74/webdav/, hxxps[://]fxbulls[.]ru, hxxps[://]fxbulls[.]ru/wp-content/uploads, hxxps[://]fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]htm, hxxps[://]fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]html, hxxps[://]84[.]32[.]189[.]74@0[.]0[.]0[.]80/fxbulls/net/2[.]url, hxxp[://]84[.]32[.]189[.]74/fxbulls, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29[.]jpg[.]url, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/Thumbs[.]db , hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/2[.]url , hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip , hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip/a2[.]cmd, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/b3[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/7z[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/7z[.]exe, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29s[.]jpg, hxxp[://]84[.]32[.]189[.]74/fxbulls/pictures/My2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls, hxxp[://]84[.]32[.]189[.]74/fxbulls/images, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29[.]jpg[.]url, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/Thumbs[.]db , hxxp[://]84[.]32[.]189[.]74/fxbulls/images/2[.]url , hxxp[://]84[.]32[.]189[.]74/fxbulls/images/a2[.]zip , hxxp[://]84[.]32[.]189[.]74/fxbulls/images/a2[.]zip/a2[.]cmd, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/a2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/b3[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/7z[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/7z[.]exe, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29s[.]jpg, hxxp[://]84[.]32[.]189[.]74/fxbulls/images/My2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/net, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29[.]jpg[.]url,

TYPE	VALUE
URLs	hxxp[://]84[.]32[.]189[.]74/fxbulls/net/Thumbs[.]db , hxxp[://]84[.]32[.]189[.]74/fxbulls/net/2[.]url , hxxp[://]84[.]32[.]189[.]74/fxbulls/net/a2[.]zip , hxxp[://]84[.]32[.]189[.]74/fxbulls/net/a2[.]zip/a2[.]cmd, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/a2[.]zip, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/b3[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/7z[.]dll, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/7z[.]exe, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29s[.]jpg, hxxp[://]84[.]32[.]189[.]74/fxbulls/net/My2[.]zip, hxxp[://]84[.]32[.]189[.]74/underwall/docs, hxxp[://]84[.]32[.]189[.]74/underwall/docs/7z.zip, hxxp[://]84[.]32[.]189[.]74/underwall/docs/passport.jpg.url, hxxp[://]84[.]32[.]189[.]74/underwall/docs/warop.url, hxxp[://]84[.]32[.]189[.]74/underwall/expand, hxxp[://]84[.]32[.]189[.]74/underwall/expand/7z.zip, hxxp[://]84[.]32[.]189[.]74/underwall/expand/photo_2023-12-26.jpg.url, hxxp[://]84[.]32[.]189[.]74/underwall/expand/warop.url, hxxp[://]84[.]32[.]189[.]74/underwall/society, hxxp[://]84[.]32[.]189[.]74/underwall/society/7z.zip, hxxp[://]84[.]32[.]189[.]74/underwall/society/photo_2023-12-26.jpg.url, hxxp[://]84[.]32[.]189[.]74/underwall/society/warop.url,

Patch Details

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21338

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21371

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21357

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21378

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21346

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21345

References

https://msrc.microsoft.com/update-guide/releaseNote/2024-Feb

https://techcommunity.microsoft.com/t5/exchange-team-blog/released-2024-h1-cumulative-update-for-exchange-server/ba-p/4047506

https://www.hivepro.com/threat-advisory/microsoft-fixed-83-vulnerabilities-including-two-zero-day-vulnerabilities/

https://www.hivepro.com/threat-advisory/microsofts-july-2023-patch-tuesday-addresses-5-zero-day-vulnerabilities/

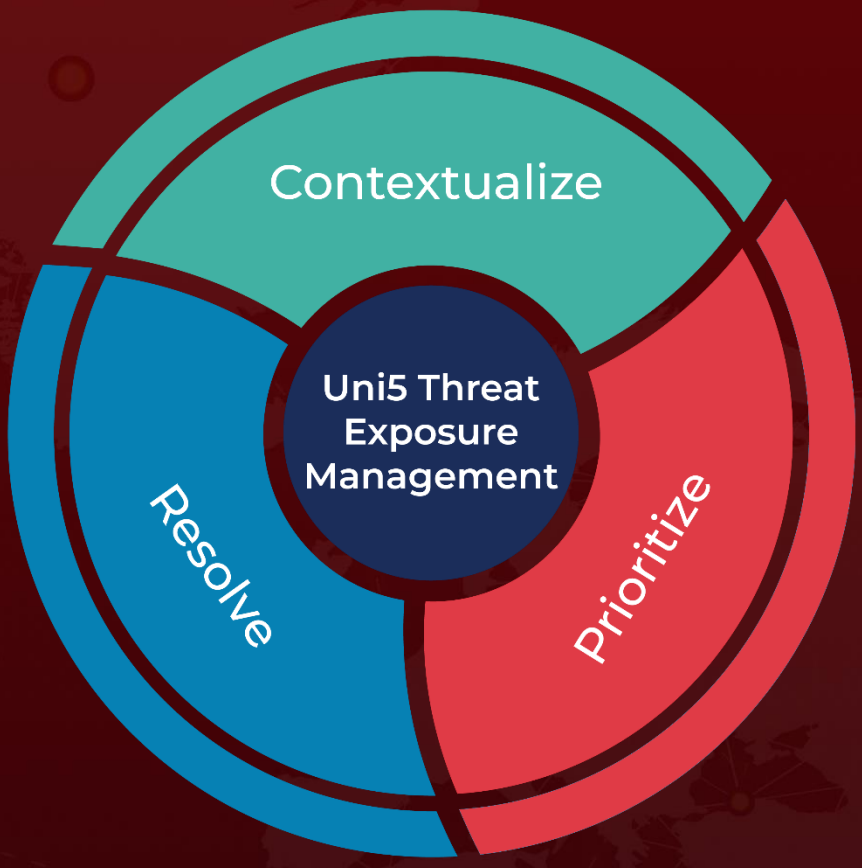
https://www.hivepro.com/threat-advisory/windows-smartscreen-exploit-paves-the-way-for-phemedrone-stealer/

https://www.hivepro.com/threat-advisory/microsoft-addresses-actively-exploited-zero-day-and-numerous-critical-flaws/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 14, 2024 • 4:30 AM

More at www.hivepro.com