Hive Pro

Threat Level

Red

CISA:AA23-074A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

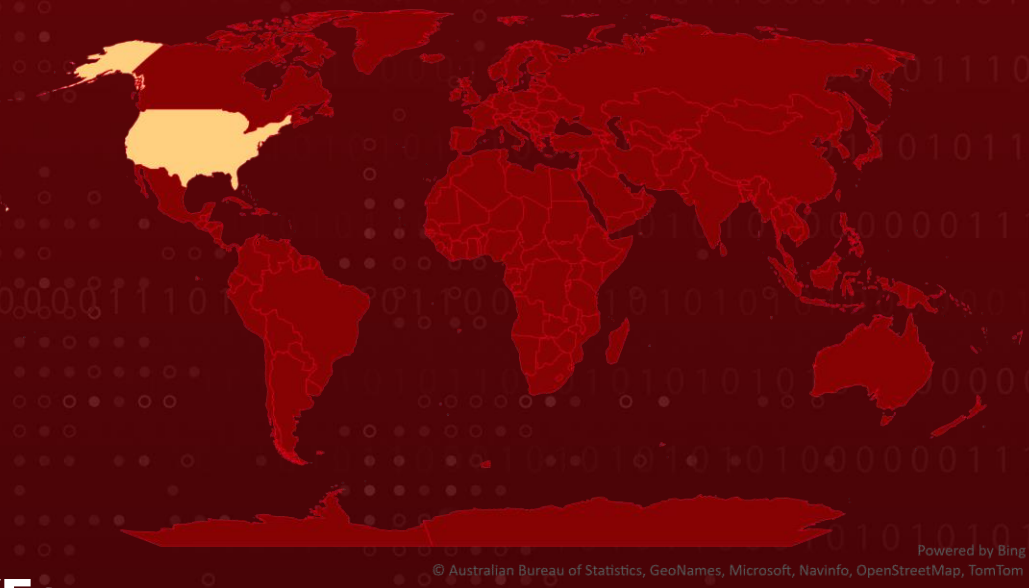
Cybercriminals Exploit Old Telerik Bug for Data Theft

Date of Publication	Admiralty Code	TA Number
June 16, 2023	A2	TA2023267

Summary

First appeared: November 2022
Attack Region: US
Targeted Sectors: Government.
Attack: APT actors and financially motivated cybercriminals were observed exploiting old Telerik vulnerabilities in an attack targeting a US government agency.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2019-18935	Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability	Telerik UI for ASP.NET AJAX	✗	✓	✓
CVE-2017-9248	Progress Telerik UI for ASP.NET AJAX and Sitefinity Cryptographic Weakness Vulnerability	ASP.NET AJAX and Sitefinity	✗	✓	✓
CVE-2017-11357	Telerik UI for ASP.NET AJAX Insecure Direct Object Reference Vulnerability	Telerik User Interface (UI) for ASP.NET AJAX	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-11317	Telerik UI for ASP.NET AJAX Unrestricted File Upload Vulnerability	Telerik User Interface (UI) for ASP.NET AJAX	✗	✓	✓

Attack Details

#1

Between November 2022 and early January 2023, several adversaries, including an advanced persistent threat (APT) actor, managed to exploit a .NET deserialization vulnerability (CVE-2019-18935) present in the Progress Telerik user interface (UI) for ASP.NET AJAX. This vulnerability was found within the Microsoft Internet Information Services (IIS) web server belonging to a federal civilian executive branch (FCEB) agency. Exploiting this vulnerability successfully enabled remote code execution.

#2

Despite having the appropriate plugin for CVE-2019-18935, the vulnerability scanner failed to detect the exploit because it overlooked the Telerik UI software installed in an atypical file path, which falls outside its usual scanning scope. This situation is not uncommon, as file paths can significantly vary depending on the organization and installation method employed.

#3

Apart from CVE-2019-18935, the version (2013.2.717) of Telerik UI for ASP.NET AJAX in question also harbors other known vulnerabilities: CVE-2017-11357, CVE-2017-11317, and CVE-2017-9248. To exploit CVE-2019-18935, the attackers must obtain the encryption keys responsible for safeguarding Telerik UI's serialization on the target system. This can be achieved by exploiting an alternate vulnerability in the target web application or leveraging CVE-2017-11317 and CVE-2017-11357.

#4

Speculation is rife regarding the intrusion of a federal agency and the subsequent data theft, with multiple cyber threat actors suspected of involvement. Among them are an advanced persistent threat (APT) actor, as well as notorious cybercriminal entities such as XE Group and Blue Mockingbird.

#5

XE Group, identified as a cybercrime syndicate believed to operate from Vietnam, has been active since at least 2013 and has a history of targeting websites hosted on IIS servers in payment card skimming schemes. Meanwhile, Blue Mockingbird appears to be capitalizing on the same vulnerability to execute attacks against United States government agencies, employing tactics reminiscent of their previous operations.

Recommendations

Validate Vulnerability Scanning Configuration: Enhance vulnerability scanning protocols to encompass atypical file paths and ensure comprehensive coverage, reducing the likelihood of overlooking crucial vulnerabilities similar to the one exploited by the cyber threat actors.

Establish Robust Patch Management and Service Account Policies: Implement a robust patch management solution to ensure timely compliance with the latest security patches. Additionally, validate the output from patch management and vulnerability scanning, cross-checking against running services to identify discrepancies and ensure comprehensive coverage. Furthermore, enforce a policy that limits service accounts to the minimum necessary permissions required for running services, minimizing potential risks and unauthorized access.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**T1595** Active Scanning	**T1595.002** Vulnerability Scanning
T1190 Exploit Public-Facing Application	**T1505** Server Software Component	**T1505.003** Web Shell	**T1036** Masquerading
T1036.005 Match Legitimate Name or Location	**T1055** Process Injection	**T1055.001** Dynamic-link Library Injection	**T1070** Indicator Removal
T1070.004 File Deletion	**T1070.006** Timestomp	**T1140** Deobfuscate/Decode Files or Information	**T1083** File and Directory Discovery
T1016 System Network Configuration Discovery	**T1105** Ingress Tool Transfer	**T1095** Non-Application Layer Protocol	**T1583** Acquire Infrastructure
T1583.003 Virtual Private Server	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.006** Python
T1505 Server Software Component	**T1505.003** Web Shell	**T1105** Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	137.184.130[.]162 45.77.212[.]12 104.225.129[.]102 149.28.85[.]24 185.186.245[.]72 193.8.172[.]113 193.8.172[.]13 216.120.201[.]12 5.34.178[.]246 79.133.124[.]242 92.38.169[.]193 92.38.176[.]109 92.38.176[.]130 144.96.103[.]245 184.168.104[.]171
Domains	xework[.]com xegroups[.]com hivnd[.]com xework[.]com
Filenames	XEReverseShell.exe Multi-OS_ReverseShell.exe SortVistaCompat
SHA256	f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4 e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913 dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2 d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35 b4222cffcdb9fb0eda5aa1703a067021bedd8cf7180cdfc5454d0f07d7eaf18f a14e2209136dad4f824c6f5986ec5d73d9cc7c86006fd2ceabe34de801062f6b a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c 8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505

TYPE	VALUE
SHA256	853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa 833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d 815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f 78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933 74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730 72f7d4d3b9d2e406fa781176bd93e8deee0fb1598b67587e1928455b66b73911 707d22cacdbd94a3e6dc884242c0565bdf10a0be42990cd7a5497b124474889b 5cbba90ba539d4eb6097169b0e9acf40b8c4740a01ddb70c67a8fb1fc3524570 508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370 1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2 144492284bcbc0110d34a2b9a44bef90ed0d6cda746df6058b49d3789b0f851d 11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad 11415ac829c17bd8a9c4cef12c3fbc23095cbb3113c89405e489ead5138384cd 08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
SHA1	f57d14e291eba19ce484ec4702a7e1f67eaeb7a0 f2dee8aa01f39543abe8d887cdeb301aa6a13088 e1bb93514f221e5c7ab14eb7793eebd4b10c9008 e12c91e1f30740ed95b9a005c8d7bd17c57d0665 db086131afaec88f4a4daa23973d214d666d39c0 d5cdda25247c3e6f1fd099077fae156ed7bada4f a7fc982d1fc30548cbe43cf643be22a31323f23b 7d6a87fa147d36ec7c46fddbb42ba7665f502207 7d165f6029eae067785fdb9af53385170d790e52 7b195c18042ab5c3ed9ebdc66800aec39e29f726 76df69648631be3c6262d6e51f066d397563f097 6b2cf97aa2adb09badbe571a4ff93bcd2398c399 6a2291e077c476d03ffe98b6f3228c82c5b451e4 679a6b4b7fa0978e38b327e318059c26b883b064 5ca0fcea7c0a4e12081cc5848ea74fd7933c599c 533bfde3f801f7e1c7b519dcb07e7f21e6546306 490a804022bcf79688422821df6012c429cec391

TYPE	VALUE
SHA1	395c45a16e491652b53b845cc3618cfe2c022f09 3489d69540a435df50e9d5d80fb59c3c3a0080b4 342e7fe54de2a60bbb82d29af375385d4ba335fe 2ec08e86c5605c1d5b4b979067148c5e4d334979 161435d198f3dba6ac1ce045b73ccd61f7697146 1228a2269610fcd20d6b0cf982b759b4c7612f34 02df1d2e88a8317215e34cb248b5a0f7a0af830a
MD5	fdef4ea27c8634c9aa94f1a16844d62c,f968639a4840535a6ecda1cb e3065260,f6f47911ac32afd786a765dcb1f26722,eaa579d911b8a47 eaaea744d59d14708,ded299dfdd68608084b8183c6d48b7a5,d8588 0ad1e87c4266f899eca02207dd4,d75ab9cb786b6f125e4cdbc92a73f a21,d3cf1d590b2a63ae6070dd0011390f03,cf96a7d57a2e28c288c7 5d371ca06f19,cece36ea4e328f093517ff68d0ed085c,ce8481189008 d7f4a685615508110d88,cd6c11f89b392988e0de3ffe048a561b,c11 27046e07137180c41cc1914e52ee7,bf6722f2055b13a61dfb7233af8 d966a,bad264a0529cacea56a845bd9d11d55b,98b5138868793006 79d634fa4e1cd27e,8e33e1e407fc9ff537b63be3ab78cb40,7947ce8 6923d732e6963c79aea757036,75221233a7dd7c5084a7d57084fd8 d43,42d7b2e1bcf75f9c469afa340f078c86,37e173b932596af62fefc4 dc10c8551d,15abeb0916a402a107c401056ebf5ac6,137423d7b7f5a 5684a9b1457f46fdfb2,0bcceb4fdfb12db21fdfc3a42b9c4693

Patch Links

https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/common-allows-javascriptserializer-deserialization

https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/common-cryptographic-weakness

https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/asyncupload-insecure-direct-object-reference

https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/asyncupload-unrestricted-file-upload

References

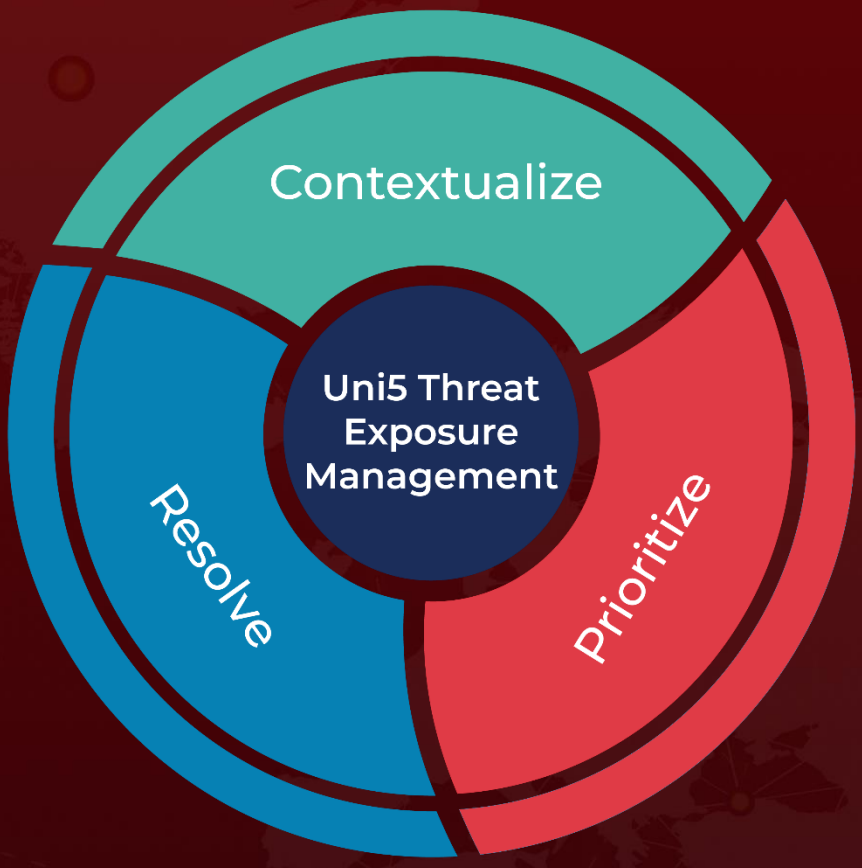
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-074a

https://news.sophos.com/en-us/2022/06/15/telerik-ui-exploitation-leads-to-cryptominer-cobalt-strike-infections/

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

June 16, 2023 • 7:31 AM

More at www.hivepro.com