FORTINET

OUTBREAK ALERTS

Progress Telerik UI Attack

Older vulnerabilities still being targeted in the wild

https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/common-allows-javascriptserializer-deserialization
CVEs: CVE-2019-18935, CVE-2017-11317, CVE-2017-11357

Versions prior to R1 2020 (2020.1.114) are susceptible to remote code execution attacks on affected web servers of Telerik User Interface (UI) for ASP.NET due to a deserialization vulnerability found in RadAsyncUpload function. FortiGuard Labs continue seeing high exploitation activity of these old vulnerabilities.

Background

Telerik UI for ASP.NET is a popular UI component library for ASP.NET web applications. In 2017, several vulnerabilities were discovered, potentially resulting in remote code execution. Attacker has to chain exploits for unrestricted file upload (CVE-2017-11317, CVE-2017-11357) and insecure deserialization (CVE-2019-18935) vulnerabilities to execute arbitrary code on a remote machine. Previously, there were two malware campaigns associated with Progress Telerik UI Attack. Netwalker Ransomware and Blue Mockbird Monero Cryptocurrency-mining. CVE 2019-18935 also made it to CISA's top routinely exploited vulnerability list in the year 2020. Even though these are old vulnerabilities attackers may still leverage them to conduct malicious activity.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a

Announced

November 03, 2021: (CVE-2019-18935) Telerik UI for ASP.NET, Deserialization Bug added to CISA known exploitation catalog
April 11, 2022: (CVE-2017-11317) Telerik UI for ASP.NET, Unrestricted File Upload Vulnerability added to CISA known exploitation catalog
January 26, 2023: (CVE-2017-11357) Telerik UI for ASP.NET, Insecure Direct Object Reference Vulnerability added to CISA known exploitation catalog

Latest Developments

March 8, 2023: FortiGuard labs research indicates high exploitation activity and IPS detections of up-to-more than 50,000+ unique IPS devices. Admins should update to the most recent version of Telerik UI for ASP.NET AJAX (at least 2020.1.114 or later) to mitigate the issue completely.
March 15, 2023: CISA released a cybersecurity advisory; Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-074a

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure

Detects and blocks Progress Telerik UI Attack and any lateral movement on the network segment

FortiDeceptor
v3.3+

Decoy VM

Detects and blocks Progress Telerik UI Attack and any lateral movement on the network segment

FortiDeceptor
v3.3+

Weaponization

Delivery

AV

Detects and blocks malware related to Progress Telerik UI Attack (CVE-2019-18935, CVE-2017-11317, CVE-2017-11357)

FortiGate *DB 91.01272*
FortiWeb *DB 91.01272*
FortiClient *DB 91.01272*
FortiSASE *DB 91.01272*
FortiMail *DB 91.01272*
FortiCASB *DB 91.01272*
FortiCWP *DB 91.01272*
FortiADC *DB 91.01272*
FortiProxy *DB 91.01272*

Vulnerability

Detects vulnerable Telerik UI For ASP NET AJAX

FortiClient *DB 1.290*

AV (Pre-filter)

Detects and blocks malware related to Progress Telerik UI Attack (CVE-2019-18935, CVE-2017-11317, CVE-2017-11357)

FortiSandbox *DB 91.01272*

Exploitation

IPS

Detects and blocks Progress Telerik UI Attack (CVE-2019-18935, CVE-2017-11317, CVE-2017-11357)

FortiGate *DB 15.838*
FortiSASE *DB 15.838*
FortiNDR *DB 15.838*
FortiADC *DB 15.838*
FortiProxy *DB 15.838*

Web App Security

Detects and blocks malware related to Progress Telerik UI Attack (CVE-2019-18935, CVE-2017-11317, CVE-2017-11357)

FortiWeb *DB 0.00344*
FortiADC *DB 1.00042*

Installation

Post-execution

Behaviour Detection engine detects unkown malware related to Progress Telerik UI Attack

FortiEDR
v4.0+

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

FortiAnalyzer *DB 0.02452*
FortiSIEM *DB 0.02452*
FortiSOCaaS *DB 0.02452*

Outbreak Detection

FortiAnalyzer *DB 1.00091*

Threat Hunting

FortiAnalyzer *v6.4+*
FortiSIEM *v6.6+*

Content Update

FortiSIEM *DB 313*

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response
FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating
FortiRecon: EASM

Additional Resources

Security Magzine
https://www.securitymagazine.com/articles/95736-us-uk-and-australia-issue-joint-cybersecurity-advisory-on-top-targeted-vulnerabilities

Bleeping Computer
https://www.bleepingcomputer.com/news/security/fbi-warns-of-netwalker-ransomware-targeting-us-government-and-orgs/

ThreatPost
https://threatpost.com/blue-mockingbird-monero-mining/155581/

ZDnet
https://www.zdnet.com/article/thousands-of-enterprise-systems-infected-by-new-blue-mockingbird-malware-gang/

Learn more about FortiGuard Outbreak Alerts

FORTINET