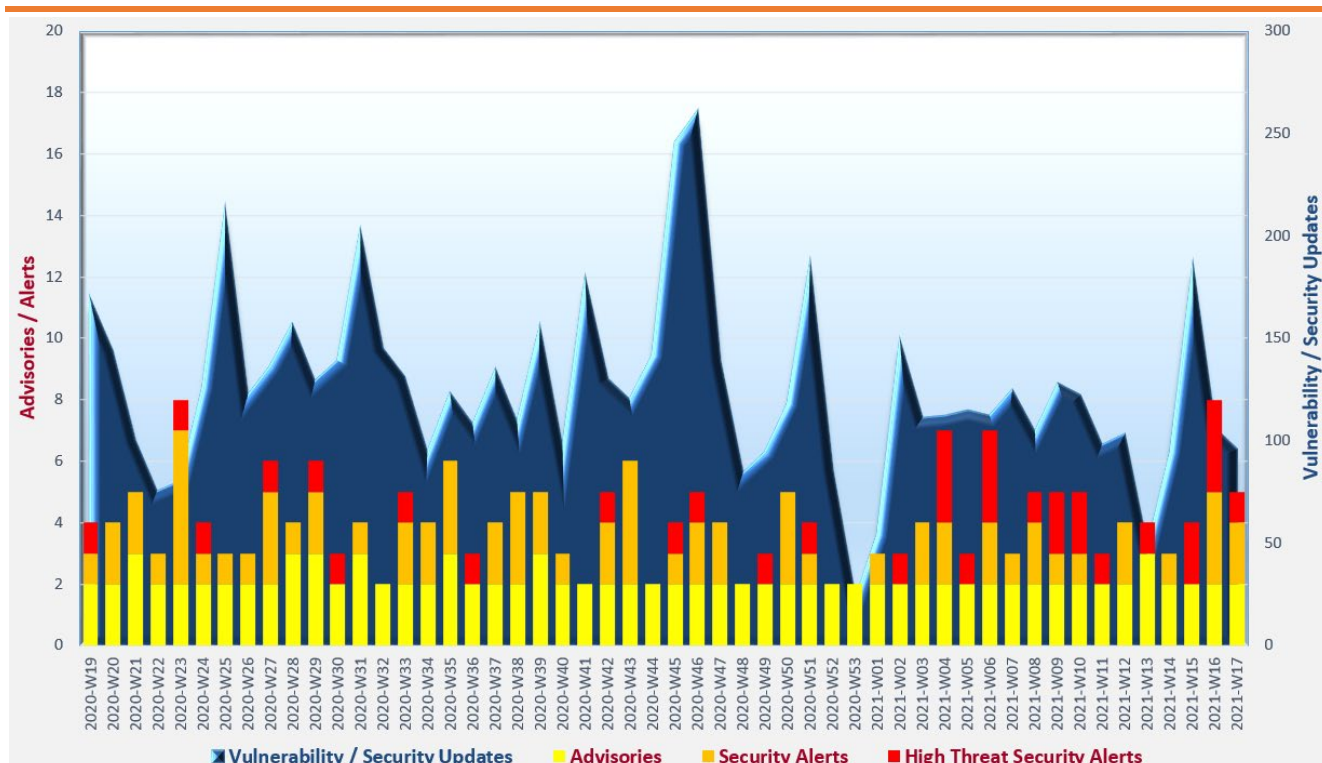


# Cyber Security Threat Trends 2021-M04

April 2021

With reference to the FIRST Traffic Light Protocol (TLP) standard<sup>1</sup>, this document is classified as **TLP:WHITE** information. Recipients may share with peers and partner organisations without restriction.

## Cyber Security Threat Landscape of the past 12 months (source: GovCERT.HK)



### Trending:

- ✧ Security risks associated with **vulnerable or outdated open source or third-party libraries** are easily overlooked by organisations. Organisations should maintain an updated inventory of third-party components used in their applications, as well as review and update those components with known vulnerabilities regularly.
- ✧ **Vulnerabilities of Virtual Private Network (VPN) solutions or remote management utilities** are increasingly targeted by attackers. System administrators should install security patches on a timely basis, shut down unnecessary network ports and services to reduce attack surfaces, and implement multi-factor authentication to strengthen the authentication control.
- ✧ **Bad bot traffic** related to malicious activities reaches a new high. Organisations should ensure that their websites have sufficient security measures and system resources to handle bot traffic. Monitoring and blocking mechanisms should be in place to detect and defend against bad bots.

<sup>1</sup> <https://www.first.org/tlp/>

## CERT Advisories



### Active exploitation of vulnerabilities in various products

CERT bodies issued alerts regarding active exploitation against vulnerabilities in various products. **System administrators should refer to vendors' documentation, apply system patches and perform mitigation measures immediately.**

- HKCERT<sup>2</sup> and JPCERT<sup>3</sup> issued alerts regarding multiple vulnerabilities in Trend Micro products such as Apex One, Apex One as a Service and OfficeScan. The vulnerability (CVE-2020-24557) was being actively exploited. Successful exploitation allows an attacker to escalate the privilege, disable security features, or abuse certain Windows features.
- GovCERT.HK<sup>4</sup>, HKCERT<sup>5</sup>, SingCERT<sup>6</sup>, CERT NZ<sup>7</sup> and Cybersecurity and Infrastructure Security Agency (CISA)<sup>8</sup> issued alerts regarding multiple vulnerabilities in Microsoft products. An Elevation of Privilege vulnerability (CVE-2021-28310) was being exploited in the wild. In addition, there were four critical Remote Code Execution (RCE) vulnerabilities in Microsoft Exchange Server 2013, 2016 and 2019 which, upon exploitation, could allow attackers gaining access to targeted systems.
- GovCERT.HK<sup>9</sup>, HKCERT<sup>10</sup>, JPCERT<sup>11</sup>, SingCERT<sup>12</sup>, CERT NZ<sup>13</sup>, Canadian Centre for Cyber Security<sup>14</sup>, and CISA<sup>15</sup> issued alerts regarding a Remote Code Execution vulnerability (CVE-2021-22893) in Pulse Connect Secure (PCS) version 9.0R3 or above. The vulnerability, together with other vulnerabilities (CVE-2019-11510, CVE-2020-8260 and CVE-2020-8243), were being actively exploited. Patch for CVE-2021-22893 was not available yet when the alerts were published. The vendor has provided workaround to mitigate the risk by **recommending system administrators to check the integrity of their appliances using the PCS Integrity Tool, and apply the security patches immediately once available.**

<sup>2</sup> [https://www.hkcert.org/security-bulletin/trend-micro-products-multiple-vulnerabilities\\_20210423](https://www.hkcert.org/security-bulletin/trend-micro-products-multiple-vulnerabilities_20210423)

<sup>3</sup> <https://www.jpccert.or.jp/english/at/2021/at210020.html>

<sup>4</sup> [https://www.govcert.gov.hk/en/alerts\\_detail.php?id=567](https://www.govcert.gov.hk/en/alerts_detail.php?id=567)

<sup>5</sup> <https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-april-2021>

<sup>6</sup> <https://www.csa.gov.sg/singcert/alerts/al-2021-023>

<sup>7</sup> <https://www.cert.govt.nz/it-specialists/advisories/updates-released-for-new-critical-vulnerabilities-in-microsoft-exchange/>

<sup>8</sup> <https://us-cert.cisa.gov/ncas/current-activity/2021/04/13/apply-microsoft-april-2021-security-update-mitigate-newly>

<sup>9</sup> [https://www.govcert.gov.hk/en/alerts\\_detail.php?id=570](https://www.govcert.gov.hk/en/alerts_detail.php?id=570)

<sup>10</sup> [https://www.hkcert.org/security-bulletin/pulse-connect-secure-zero-day-remote-code-execution-vulnerability\\_20210422](https://www.hkcert.org/security-bulletin/pulse-connect-secure-zero-day-remote-code-execution-vulnerability_20210422)

<sup>11</sup> <https://www.jpccert.or.jp/english/at/2021/at210019.html>

<sup>12</sup> <https://www.csa.gov.sg/singcert/alerts/al-2021-027>

<sup>13</sup> <https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-pulse-connect-secure-actively-exploited/>

<sup>14</sup> <https://www.cyber.gc.ca/en/alerts/active-exploitation-pulse-connect-secure-vulnerabilities>

<sup>15</sup> <https://us-cert.cisa.gov/ncas/alerts/aa21-110a>

## CERT Advisories

- GovCERT.HK<sup>16</sup>, HKCERT<sup>17</sup>, SingCERT<sup>18</sup>, CERT NZ<sup>19</sup> and CISA<sup>20</sup> issued alerts regarding multiple vulnerabilities in SonicWall Email Security products (version 10.0.9 and earlier). Three zero-day vulnerabilities (CVE-2021-20021, CVE-2021-20022 and CVE-2021-20023) were being exploited in the wild. Successful exploitation could allow the attacker to take full control over the targeted system.
- SingCERT<sup>21</sup>, CISA<sup>22</sup>, Canadian Centre for Cyber Security<sup>23</sup>, Australian Cyber Security Centre (ACSC)<sup>24</sup> and National Cyber Security Centre (NCSC)<sup>25</sup> issued alerts regarding multiple vulnerabilities in Fortinet FortiOS. A number of vulnerabilities (CVE-2018-13379, CVE-2020-12812 and CVE-2019-5591) were being actively exploited for gaining access to targeted networks.
- HKCERT<sup>26</sup>, SingCERT<sup>27</sup> and CERT NZ<sup>28</sup> issued alerts regarding multiple vulnerabilities in QNAP Network Attached Storage (NAS) devices. Two vulnerabilities (CVE-2020-36195 and CVE-2021-28799) were being actively exploited to deploy ransomware (Qlocker and eCh0raix) in vulnerable systems.



### GovCERT.HK Annual Report 2020

GovCERT.HK published the GovCERT.HK Annual Report 2020<sup>29</sup>, providing information on its achievements in 2020 on various areas including Cyber Security Information Sharing, Cyber Threat Intelligence Management, Government IT Security Policy and Guidelines, Liaison and Collaboration, Awareness Building and Public Education, etc. and related statistics.

<sup>16</sup> [https://www.govcert.gov.hk/en/alerts\\_detail.php?id=572](https://www.govcert.gov.hk/en/alerts_detail.php?id=572)

<sup>17</sup> [https://www.hkcert.org/security-bulletin/sonicwall-email-security-multiple-zero-day-vulnerabilities\\_20210421](https://www.hkcert.org/security-bulletin/sonicwall-email-security-multiple-zero-day-vulnerabilities_20210421)

<sup>18</sup> <https://www.csa.gov.sg/singcert/alerts/al-2021-028>

<sup>19</sup> <https://www.cert.govt.nz/it-specialists/advisories/vulnerabilities-in-sonicwall-email-security-actively-exploited/>

<sup>20</sup> <https://us-cert.cisa.gov/ncas/current-activity/2021/04/21/sonicwall-releases-patches-email-security-products>

<sup>21</sup> <https://www.csa.gov.sg/singcert/alerts/al-2021-022>

<sup>22</sup> <https://us-cert.cisa.gov/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios>

<sup>23</sup> <https://www.cyber.gc.ca/en/alerts/exploitation-fortinet-fortios-vulnerabilities-cisa-fbi>

<sup>24</sup> <https://www.cyber.gov.au/acsc/view-all-content/alerts/apt-exploitation-fortinet-vulnerabilities>

<sup>25</sup> <https://www.ncsc.gov.uk/news/critical-risk-unpatched-fortinet-vpn-devices>

<sup>26</sup> [https://www.hkcert.org/security-bulletin/qnap-nas-security-restriction-bypass-vulnerability\\_20210423](https://www.hkcert.org/security-bulletin/qnap-nas-security-restriction-bypass-vulnerability_20210423)

<sup>27</sup> <https://www.csa.gov.sg/singcert/alerts/al-2021-029>

<sup>28</sup> <https://www.cert.govt.nz/it-specialists/advisories/qnap-nas-vulnerabilities-exploited-to-deploy-ransomware/>

<sup>29</sup> <https://www.govcert.gov.hk/en/annualreport.html>

---

## CERT Advisories

---



### Social media users should stay alert and review their accounts regularly

Regarding recent data leakage incidents on social media platforms, HKCERT<sup>30</sup>, SingCERT<sup>31</sup>, CERT NZ<sup>32</sup> and MyCERT<sup>33</sup> issued advisories reminding social media users to stay vigilant to social engineering activities, personalised scams, or phishing attacks potentially arose from the breaches. The leaked information included user profile name, date of birth, email address, phone number, etc. Apart from social engineering attacks, users should be cautious about unsolicited phone calls, as well as messages sent over SMS or instant messaging applications. In addition, they should review the privacy settings, permissions, and data shared online regularly.



### Security tips for protecting WhatsApp account

HKCERT<sup>34</sup> published an article to help users to protect their WhatsApp accounts from unauthorised deactivation. Actionable security tips included enable two-step verification and provide email address (even though it is optional); report to WhatsApp immediately if abnormal SMS verification code is received; use lost tracking feature to lock the mobile phone or remotely wipe the mobile phone data if the mobile phone is lost, etc.



### Guidance on cyber security measures for high profile conferences

NCSC<sup>35</sup> published a guidance for event organisers of high profile conferences. The guidance helped the organisers to understand the cyber risks such as denial of service attacks, disruption by uninvited guests, compromised suppliers, venue-related issues, etc. Protective measures such as threat monitoring were also provided for reference.

---

<sup>30</sup> <https://www.hkcert.org/blog/protect-sensitive-information-in-the-use-of-social-media-and-beware-of-potential-cyber-attacks-arising-from-data-leakages>

<sup>31</sup> <https://www.csa.gov.sg/singcert/advisories/ad-2021-004>

<sup>32</sup> <https://www.cert.govt.nz/individuals/alerts/facebook-data-leak-publicly-available/>

<sup>33</sup> <https://www.mycert.org.my/portal/advisory?id=MA-803.042021>

<sup>34</sup> <https://www.hkcert.org/blog/beware-of-unauthorised-deactivation-of-whatsapp-account>

<sup>35</sup> <https://www.ncsc.gov.uk/guidance/cyber-security-for-high-profile-conferences>

## Industry Insight on Cyber Security Threat Trends

### Rise of unpatched, outdated or abandoned open source libraries in organisations

Synopsys assessed and analysed the anonymised audit findings from 1,546 commercial codebases in 17 industries, and published the study results in its "2021 Open Source Security and Risk Analysis Report"<sup>36</sup>. The major observations in the report were:

- **98% of the audited codebases contained at least one open source component.** On average, 528 open source components were found per codebase. **Organisations were recommended to identify and take inventory for all open source and third-party components used in each application to have a complete visibility on the components used.**
- **84% of assessed codebases were found with at least one known open source security vulnerability, increased from 75% in 2019.** Percentage of assessed codebases with high-risk open source vulnerabilities also increased to 60% in 2020 from 49% in 2019. Almost 158 vulnerabilities per codebase were uncovered in average. **Organisations should conduct penetration test and source code scan to identify vulnerabilities in their Internet-facing systems regularly.**
- **Timely patching or update of open source components was not in place.** The average age of vulnerabilities identified was around 2.2 years. The top four open source vulnerabilities that were found in codebases in 2020 also presented in the 2019 audits, with percentage increases ranging from 4% to 16%. **Organisations should also note the patch delivery mechanism of the open source components they used, which could be different from the "push" mechanism adopted in some commercial software.**
- **Usage of aging or abandoned open source components was alarming.** 85% of the assessed codebases contained components outdated for more than four years. Components without development activity or security patch in the past two years were found in 91% of the audited codebases. **Organisations should set and review the vulnerability patching priorities, with consideration on the business importance and the criticality of the asset, as well as the risk of exploitation.**
- **Around 95% of audited applications in the marketing technology industry were found with vulnerable dependent open source components.** Percentage of codebases with vulnerable open source components in industries such as energy and clean technology, enterprise software / SaaS, retail and e-commerce, financial services and FinTech, healthcare and Internet of Things was between 60% and 80%.

Source: Synopsys

<sup>36</sup> <https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html>

---

## Industry Insight on Cyber Security Threat Trends

---

### COVID-19 themed threats still soared in the second half of 2020

McAfee published the report “McAfee Labs Threats Report”<sup>37</sup>, which summarised their analysis on threats identified in the second half of 2020. The major observations were:

- **COVID-19 themed threats doubled in Q3 2020 with over 1.07 million detections as compared to Q2 2020 (around 0.45 million detections) and further increased by 14% in Q4 2020 to more than 1.22 million detections.**
- **Number of new malware detections rose continuously in 2020.** On average, 648 threats were detected per minute in Q4 2020, accounted for a growth of 10% as compared to Q3 2020 (588 threats per minute). New Powershell threats in Q4 2020 surged with a 208% increase as compared to Q3 2020. New Office malware, mobile malware and ransomware also soared significantly from Q3 to Q4. There was a spike in new MacOS malware detection in Q3 2020 due to EvilQuest ransomware. On the other hand, new Coin Miner malware, IoT malware and Javascript malware decreased continuously in H2 2020.
- **Security incidents targeted the public sector almost doubled in Q4 2020 as compared to Q3 2020.** There was also a notable increase in publicly disclosed security breaches targeted the healthcare sector in the second half of 2020. Malware was the dominant attack vector for publicly disclosed security breaches in 2020.
- **New Ransomware detections surged in the second half of 2020 with over 5 million detections in Q4 2020.** More than half of the detections belonged to REvil ransomware family. Other prevalent ransomware families included Thanos, Ryuk, RansomeXX, and Maze. Attackers increasingly switched from spray-and-pay approach to attacking high-value targets and exfiltrated the victims’ data in addition to traditional encrypting data for ransom.
- **There was an increasing trend that cyber criminals proactively utilised vulnerabilities in external facing applications including Virtual Private Network (VPN) solutions or remote management utilities to gain initial access for launching attacks.** Attackers also continued to improve the evasion capability of malware, for instance, some malicious payload were found embedded within virtual hard disk (VHD) files to elude detection in Q4 2020.

*Source: McAfee*

---

<sup>37</sup> <https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html>

## Industry Insight on Cyber Security Threat Trends

### Bad bot traffic hits an historical high in 2020

Imperva published its “2021 Bad Bot Report”<sup>38</sup> which presented the analysis results on bot activities in the application layer and website security based on the data collected from their network in 2020. The highlights from the report included:

- **25.6% of Internet traffic was bad bot traffic, increased by 6.2% in 2020 and reached a record high.** These bad bots performed malicious activities such as unauthorised web scraping, scalping, fraud, account takeover attacks, etc. **3.5% of bad bot traffic targeted Hong Kong, making Hong Kong the 6th most attacked location in 2020.**
- **57.1% of bad bots were advanced persistent bots of different sophistication.** They could be headless browsers or real browsers with malware installed, and were capable of executing JavaScript or generating mouse movements and clicks to imitate human activities. They accessed target sites through random IP addresses, anonymous proxies or peer-to-peer networks, used different user agent strings, and generated low request volume and frequency to evade detection. **Organisations could consider blocking traffic from hosting providers and proxy services known for bad bot traffic to mitigate the risk.**
- **The top 3 industries with the most bad bot traffic in 2020 were Telecom & ISPs (45.7%), Computing & IT (41.1%), and Sports (33.7%).** Some industries recorded significant increase in specific period in 2020. For instance, healthcare websites recorded a 372% increase in bad bot traffic since September 2020 which could be related to offerings of vaccine appointment. Retail websites also recorded 788% increase in bad bot traffic from September to October 2020 and stayed at a high level till end of year 2020, could be due to the demand on new generation gaming consoles and holiday season shopping frenzy.
- **Bad bots with mobile browsers as client identities increased.** Although Chrome remained the most prevalent fake identity for bad bots, its usage dropped from 55.4% of the overall bad bot traffic in 2019 to 33.3% in 2020. On the other hand, bad bots using mobile user agents increased from 12.9% in 2019 to 28.1% in 2020. Bad bot traffic from mobile ISPs also increased significantly in 2020, from 2.3% in 2019 to 15.1% of all bad bot traffic in 2020. **Organisations could consider blocking traffic from outdated user agents or browsers to fend off some of bad bot attacks.**

*Source: Imperva*

---

<sup>38</sup> <https://www.imperva.com/resources/resource-library/reports/bad-bot-report/>



## Summary of Microsoft April 2021 Security Updates

# 11

Product Families  
with Patches

# 5

Critical

# 6

Important or  
below

Product Family	Impact <sup>39</sup>	Severity	Associated KB and / or Support Webpages
<b>Windows 10</b>	Remote Code Execution	Critical ★★★★	<a href="#">KB5001330</a> , <a href="#">KB5001337</a> , <a href="#">KB5001339</a> , <a href="#">KB5001340</a> , <a href="#">KB5001342</a> , <a href="#">KB5001347</a>
<b>Windows Server 2016, 2019 and Server Core installations</b>	Remote Code Execution	Critical ★★★★	<a href="#">KB5001330</a> , <a href="#">KB5001337</a> , <a href="#">KB5001342</a> , <a href="#">KB5001347</a>
<b>Windows 8.1 and Windows Server 2012, 2012 R2</b>	Remote Code Execution	Critical ★★★★	<a href="#">KB5001382</a> , <a href="#">KB5001383</a> , <a href="#">KB5001387</a> , <a href="#">KB5001393</a>
<b>Microsoft Exchange Server</b>	Remote Code Execution	Critical ★★★★	<a href="#">KB5001779</a>
<b>Azure</b>	Remote Code Execution	Critical ★★★★	Azure DevOps Server 2020 and 2020.0.1: <a href="#">Release Notes</a> Azure DevOps Server 2019 Update 1.1: <a href="#">Release Notes</a> Azure DevOps Server 2019 Update 1: <a href="#">Release Notes</a> Azure DevOps Server 2019 Update 0.1: <a href="#">Release Notes</a> Azure Sphere: <a href="#">CVE-2021-28460</a> <a href="#">@azure/ms-rest-nodeauth</a> : <a href="#">Release Notes</a>
<b>Microsoft Office-related software</b>	Remote Code Execution	Important ★★★	<a href="#">KB2553491</a> , <a href="#">KB2589361</a> , <a href="#">KB3178639</a> , <a href="#">KB3178643</a> , <a href="#">KB4493215</a> , <a href="#">KB4504722</a> , <a href="#">KB4504724</a> , <a href="#">KB4504726</a> , <a href="#">KB4504727</a> , <a href="#">KB4504738</a> , <a href="#">KB4504739</a> Microsoft Excel: <a href="#">KB3017810</a> , <a href="#">KB4504721</a> , <a href="#">KB4504735</a>

<sup>39</sup> The Impact and Severity are the maximum impact and severity assessment of the vulnerabilities in the associated knowledgebase (KB) by Microsoft.




Product Family	Impact <sup>39</sup>	Severity	Associated KB and / or Support Webpages
			Microsoft Outlook: <a href="#">KB4493185</a> , <a href="#">KB4504712</a> , <a href="#">KB4504733</a> Microsoft Word: <a href="#">KB4493198</a> , <a href="#">KB4493208</a> , <a href="#">KB4493218</a> Microsoft Office Online Server: <a href="#">KB4504714</a> Microsoft Office Web Apps: <a href="#">KB4504705</a> , <a href="#">KB4504729</a> Microsoft Office 2019 for Mac: <a href="#">Release Notes</a> Microsoft Office 2019: <a href="#">Click to Run</a> Microsoft 365 Apps for Enterprise: <a href="#">Click to Run</a>
Microsoft SharePoint-related software	Remote Code Execution	Important ★★★	<a href="#">KB4493170</a> , <a href="#">KB4493201</a> , <a href="#">KB4504701</a> , <a href="#">KB4504709</a> , <a href="#">KB4504715</a> , <a href="#">KB4504716</a> , <a href="#">KB4504719</a> , <a href="#">KB4504723</a>
Microsoft Visual Studio	Remote Code Execution	Important ★★★	Microsoft Visual Studio 2015 Update 3: <a href="#">KB5001292</a> Microsoft Visual Studio 2017 version 15.9: <a href="#">Release Notes</a> Microsoft Visual Studio 2019 version 16.4: <a href="#">Release Notes</a> Microsoft Visual Studio 2019 version 16.7: <a href="#">Release Notes</a> Microsoft Visual Studio 2019 version 16.9: <a href="#">Release Notes</a> Visual Studio Code: <a href="#">Release Notes</a> Visual Studio Code - Maven for Java Extension: <a href="#">Release Notes</a> Visual Studio Code - Kubernetes Tools: <a href="#">Release Notes</a> Visual Studio Code - GitHub Pull Requests and Issues Extension: <a href="#">Release Notes</a>
Raw Image Extension	Remote Code Execution	Important ★★★	<a href="#">CVE-2021-28466</a> , <a href="#">CVE-2021-28468</a>
Team Foundation Server	Information Disclosure	Important ★★★	Team Foundation Server 2015 Update 4.2: <a href="#">Release Notes</a>

Product Family	Impact <sup>39</sup>	Severity	Associated KB and / or Support Webpages
			Team Foundation Server 2017 Update 3.1: <a href="#">Release Notes</a> Team Foundation Server 2018 Update 1.2: <a href="#">Release Notes</a> Team Foundation Server 2018 Update 3.2: <a href="#">Release Notes</a>
<b>VP9 Video Extensions</b>	Remote Code Execution	Important ★ ★ ★	<a href="#">CVE-2021-28464</a>

Learn more:

High Threat Security Alert (A21-04-02): Multiple Vulnerabilities in Microsoft Products (April 2021)  
([https://www.govcert.gov.hk/en/alerts\\_detail.php?id=567](https://www.govcert.gov.hk/en/alerts_detail.php?id=567))

#### Sources:

 Microsoft April 2021 Security Updates  
(<https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Apr>)