verizon

Verizon Business Consulting Services
Cyber Security Consulting

Verizon Cybersecurity Solutions Intelligence Summary (INTSUM)

For the week ending 2021-03-12

Weekly Summary

Microsoft Exchange Servers have become the nexus for InfoSec risk. At least 10 threat actors have been attacking Exchange Servers to install web shells. An unknown number of actors are targeting unsecured web shells for hijacking. At least one actor is installing a new ransomware on the breached servers. Shadowserver has metrics and visualizations for compromised Exchange Servers. F5 released a security advisory to address 21 vulnerabilities impacting BIG-IP and BIG-IQ devices. Microsoft has released a total of 89 security patches in March including CVE-2021-26411 that was exploited in January by a North Korean adversary targeting security researchers. Five remote code execution vulnerabilities in Microsoft DNS Server should receive patching priority.

- *Prefaces/Tags:*

TTP: tactics, techniques and procedures	**YARA**: intelligence includes a YARA rule
SA: situational awareness	**KT:** Key takeaway(s)
IOC: network indicators of compromise (IP, FQDN, Snort IDs). Hash digests and registry keys are IOC; collections with only hashes or keys will not usually have the IOC preface. (**IOC links will be in bold**)	
(Gnnnn) (Group) **(Snnnn)** (Software) **(Tnnnn)** (Tactic/Technique) **MITRE ATT&CK ID# (beta)**	

Significant new threats

- *Summary:* The four new vulnerabilities in Microsoft Exchange and the attacks exploiting them have been nicknamed "ProxyLogon" initially by DevCore, a Taiwan-based security consulting firm. On Dec 10th, DevCore identified CVE-2021-26855 the server-side request forgery (SSRF) vulnerability in Exchange which allowed the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
  - **(TTP&IOC&YARA)** CISA | "**Alert (AA21-062A) Mitigate Microsoft Exchange Server Vulnerabilities**." CISA updated Alert AA21-062A four times since last Friday. Changes include TTP updates, updated resources and information about DearCry ransomware. Most recently, CISA published 7 Malware Analysis Reports (MAR) for China Chopper Webshells, and each MAR included a STIX file with hash values.
  - **(TTP&IOC&YARA)** Blue Team Blog | **"Microsoft Exchange Zero Day's – Mitigations and Detections,"** This is the best single collection of intelligence and resources for protecting Exchange servers, post-exploitation activities by the attackers, links to tools, scripts, YARA rules, DearCry ransomware and threat hunting resources.
  - **(SA)** Shadowserver Foundation | "HAFNIUM Exchange Victims," "Exchange Scanning #1" and "Exchange Scanning #2" Exchange scanning reports provide global metrics and data visualizations of the results. Detailed reports are available to registrants directly responsible for security of ASN or CIDR network space.
    - The Hafnium report covers victims of HAFNIUM exploitation of Exchange Server via CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 between 2021-02-26 and 2021-03-03, but not subsequent mass exploitation after the patches were released. The total dataset distributed includes over 68500 distinct IP addresses. Of these IP addresses, there is high certainty that 8911 IP addresses were compromised.

    - The Exchange #1 report covers Exchange Servers potentially vulnerable to CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 by scanning with DIVD after patches were released. The total dataset includes over 64088 unique IP addresses that were assessed on 2021-03-09 as potentially still having exposed Microsoft Exchange Server vulnerabilities.
    - The Exchange #2 report provides critical information about compromised Exchange Servers with exposed public web shells that were likely exploited using CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065. The total dataset covers 6720 unique web shell URL paths corresponding to 5818 unique IP addresses that were assessed on 2021-03-12 as being compromised Exchange Servers.
  - **(TTP&IOC)** BleepingComputer | "**Ransomware now attacks Microsoft Exchange servers with ProxyLogon exploits**," Beginning on Mar 9th, malware researchers were collecting reports of a new strain of ransomware infecting and encrypting Exchange servers.
  - **(TTP)** Microsoft Security Intelligence | "We have detected and are now blocking a new family of ransomware being used after an initial compromise of unpatched on-premises Exchange Servers," Microsoft security confirming the new malware was Ransom:Win32/DoejoCrypt.A, which is also known as DearCry. (Mar 11th)
  - **(TTP&IOC)** Palo Alto Networks Unit 42 Intelligence | **"Threat Assessment: DearCry Ransomware,"** Threat assessment of the DearCry ransomware including techniques observed and courses of action that can be used to mitigate.
  - **(SA)** "Microsoft Support Emergency Response Tool (MSERT)" | Microsoft Defender has included security intelligence updates to the latest version of the Microsoft Safety Scanner (MSERT.EXE) to detect and remediate the latest threats known to abuse the Exchange Server vulnerabilities disclosed on March 2, 2021.
  - **(TTP&IOC)** DomainTools | "**Examining Exchange Exploitation and its Lessons for Defenders**" The rapid expansion in Exchange exploitation threatens organizations large and small that are using this software. Based on the rapid expansion in activity, threat attribution and similar evaluation will be difficult if not impossible, especially as public POCs become available.
  - **(TTP&IOC)** ESET | **"Exchange servers under siege from at least 10 APT groups."** ESET found LuckyMouse (G0027), Tick (G0060), Winnti Group (G0044), and Calypso, among others, are likely using the recent Exchange vulnerabilities to compromise email servers all around the world.
  - **(TTP)** *Ars Technica* | "There's a vexing mystery surrounding the 0-day attacks on Exchange servers." The Exchange vulnerabilities that allow hackers to take over Exchange servers are under attack by no fewer than 10 advanced hacking groups, six of which began exploiting them before Microsoft released a patch, researchers reported Wednesday. That raises a vexing question: how did so many separate threat actors have working exploits before the security flaws became publicly known?

Risk-relevant vulnerabilities

- *Summary:* **(SA)** F5 | "Article: K02566623 - Overview of F5 critical vulnerabilities." F5 released a security advisory to address 21 vulnerabilities impacting BIG-IP and BIG-IQ devices. These included two critical remote code execution (RCE) vulnerabilities, CVE-2021-22986 and CVE-2021-22987 and two critical buffer overflow vulnerabilities, CVE-2021-22991 and CVE-2021-22992. An attacker could exploit these vulnerabilities to take control of an affected system. The VTRAC has no intelligence of proof of concept exploit code in the wild.
- *Summary:* **(SA)** CERT-EU | "Vulnerabilities in Microsoft DNS Server (CERT-EU Security Advisory 2021-014)" Microsoft released patches for 5 bugs listed as DNS Server Remote Code Execution (RCE) Vulnerabilities. CVE-2021-26897 is the only one Microsoft scored as Critical. Enabling Secure Zone Updates would protect from attacks on public-facing interfaces, but not from an attacker with a foothold on the network (domain-joined computer). All five vulnerabilities are listed with a CVSS=9.8.
  - McAfee | "Seven Windows Wonders – Critical Vulnerabilities in DNS Dynamic Updates." McAfee published a vulnerability assessment of the 5 RCE vulnerabilities plus 2 additional DoS vulnerabilities. McAfee assessed the RCE vulnerabilities are not wormable.