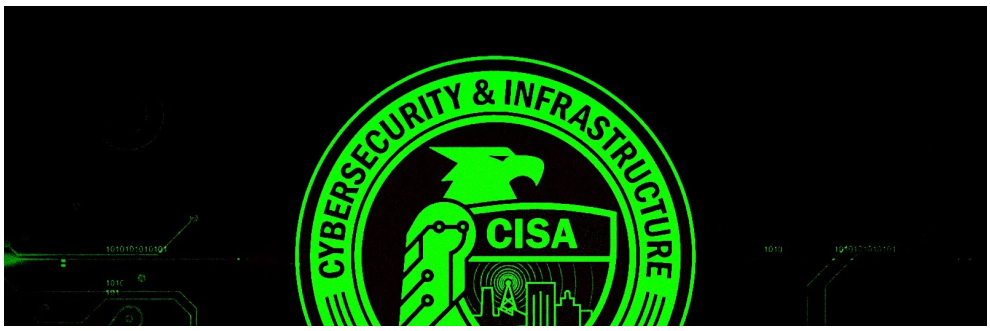
CISA urges orgs to patch actively exploited Windows SeriousSAM bug

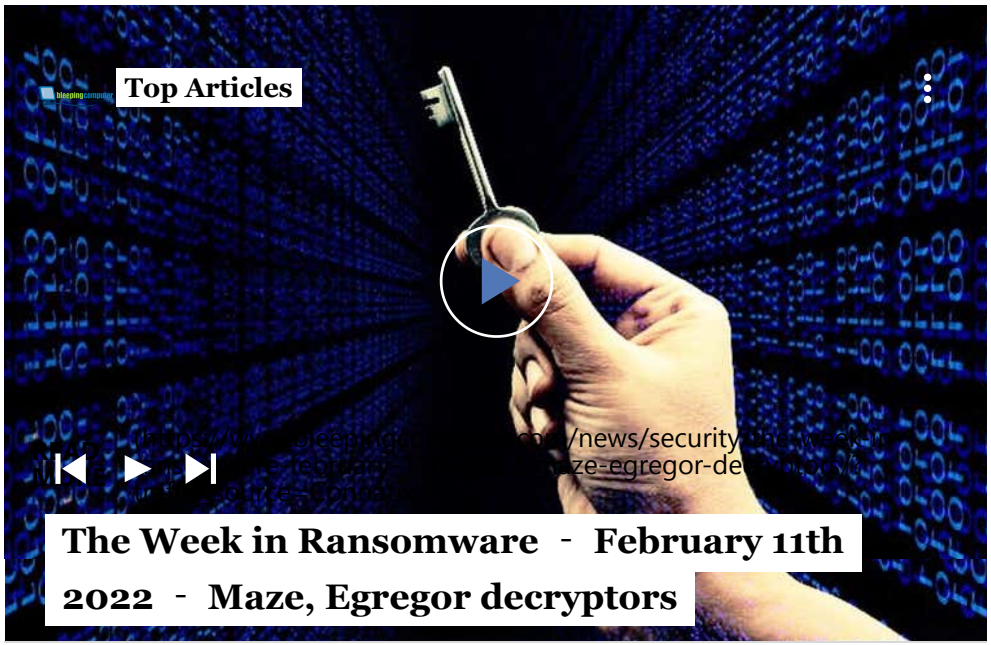
By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** February 11, 2022 08:01 AM **0**



The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has added to the catalog of vulnerabilities another 15 security issues actively used in cyberattacks.

CISA's warning about these vulnerabilities serves as a wake-up call to all system administrators that they need to prioritize installing security updates to protect their organizations' networks.

Failing to do so turns the company into a target for threat actors, who could breach digital premises, compromise data or gain access to sensitive accounts.



Among the new security flaws CISA added to the catalog of actively exploited bugs, CVE-2021-36934 is the one that stands out. This is a Microsoft Windows SAM (Security Accounts Manager) vulnerability that allows anyone to access the Registry database files on Windows 10 and 11, extract password hashes and gain administrator privileges (https://www.bleepingcomputer.com/news/microsoft/new-windows-10-vulnerability-allows-anyone-to-get-admin-privileges/).

Microsoft fixed this flaw in July 2021 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934), but seven months later there is still a significant number of systems that need to install the update. Also, there are workarounds for this vulnerability available here (https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-workaround-for-windows-10-serioussam-vulnerability/).

The 15 flaws highlighted this time (https://www.cisa.gov/uscert/ncas/current-activity/2022/02/10/cisa-

CVE-2021-36934	Microsoft Windows SAM Local Privilege Escalation Vulnerability	2/24/2022
CVE-2020-0796	Microsoft SMBv3 Remote Code Execution Vulnerability	8/10/2022
CVE-2018-1000861	Jenkins Stapler Web Framework Deserialization of Untrusted Data	8/10/2022
CVE-2017-9791	Apache Struts 1 Improper Input Validation Vulnerability	8/10/2022
CVE-2017-8464	Microsoft Windows Shell (.lnk) Remote Code Execution	8/10/2022
CVE-2017-10271	Oracle Corporation WebLogic Server Remote Code Execution	8/10/2022

CVE-2017-0263	Microsoft Win32k Privilege Escalation Vulnerability	8/10/2022
CVE-2017-0262	Microsoft Office Remote Code Execution Vulnerability	8/10/2022
CVE-2017-0145	Microsoft SMBv1 Remote Code Execution Vulnerability	8/10/2022
CVE-2017-0144	Microsoft SMBv1 Remote Code Execution Vulnerability	8/10/2022
CVE-2016-3088	Apache ActiveMQ Improper Input Validation Vulnerability	8/10/2022
CVE-2015-2051	D-Link DIR-645 Router Remote Code Execution	8/10/2022
CVE-2015-1635	Microsoft HTTP.sys Remote Code Execution Vulnerability	8/10/2022
CVE-2015-1130	Apple OS X Authentication Bypass Vulnerability	8/10/2022
CVE-2014-4404	Apple OS X Heap-Based Buffer Overflow Vulnerability	8/10/2022

Of the rest, CVE-2020-0796 is another critical security flaw on CISA's list that admins should address. The bug received the maximum severity score. It consists in erroneous handling of maliciously crafted compressed data packets by SMBv3 and it can be exploited to achieve remote code execution.

The flaw can accommodate “wormable” attacks (https://www.bleepingcomputer.com/news/security/microsoft-leaks-info-on-wormable-windows-smbv3-cve-2020-0796-flaw/), which means that a threat actor could compromise large networks quicker and with less effort.

Back in March 2020, there were at least 48,000 systems (https://www.bleepingcomputer.com/news/security/48k-windows-hosts-vulnerable-to-smbghost-cve-2020-0796-rce-attacks/) vulnerable to CVE-2020-0796, but, as underlined by CISA’s latest report, the problem continues to persist on many systems.

CISA also added CVE-2015-2051, a remote code execution bug affecting D-Link DIR-645 routers that continues to deliver to attackers.

The most recent reports of exploitation for the particular vulnerability date from November 2021, when the BotenaGo botnet (https://www.bleepingcomputer.com/news/security/botenago-botnet-targets-millions-of-iot-devices-with-33-exploits/) targeted millions of IoT devices and routers via a set of 33 known exploits, including CVE-2015-2051