From: WaterISAC <info@waterisac.org>
Sent: Thursday, March 4, 2021 12:55 PM
Subject: UPDATE: Report of Cyber Intrusion in the Sector Exploiting Microsoft Exchange Server Vulnerabilities

WATER ISAC SUPERCHARGE YOUR SECURITY

TLP:GREEN

ATTENTION: If you maintain an on-premises Microsoft Exchange server, WaterISAC encourages you to review and address/apply the information below immediately. Failure to mitigate could result in an unauthenticated attacker executing execute arbitrary code on the server to gain full access to files, mailboxes, and credentials stored on that system.

WaterISAC Members,

WaterISAC has received a report of a utility company that provides water and electric services to a small city experiencing an intrusion due to exploitation of the recently-disclosed Microsoft Exchange Server vulnerabilities. The report included IP addresses involved in the intrusion, and additional IP addresses known to be associated with this activity (listed below and in a spreadsheet posted to WaterISAC here). This information is consistent with additional intelligence indicating the activity is more widespread than initially realized, and includes victims in city and county governments, healthcare organizations, banks/financial institutions, and several residential electricity providers.

Furthermore, it is anticipated that threat actors are looking for low-hanging fruit, and will be especially more active after the disclosure over the past 36-48 hours. Additionally, researchers have detected webshells being deployed on some compromised systems. Undetected webshells provide a backdoor into networks which enable threat actors to maintain access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Webshells are used to remotely control compromised devices which often enables actors to gain access, including full control to additional network resources.

Given this development, WaterISAC urges members to investigate their networks for activity emanating from the IP addresses (which may serve as an indication of compromise). Members should consult the information and mitigation recommendations in the Alert (AA21-062A) and Emergency Directive 21-02 released by the Cybersecurity and Infrastructure Security Agency (CISA) yesterday and take the necessary steps to protect their environments from intrusions.

IP Addresses

45.155.205.225
104.248.49.97
13.231.174.2
157.230.221.198
165.232.154.116
192.81.208.169
45.76.110.29
* 5.2.69.14
161.35.45.41
45.77.252.175
103.77.192.219
104.140.114.110
104.250.191.110
108.61.246.56
149.28.14.163
167.99.168.251
185.250.151.72
203.160.69.66
211.56.98.146
5.254.43.18
80.92.205.81
*91.192.103.43

*Known Tor exit nodes

CISA Partner Call Tomorrow

CISA is hosting a call tomorrow with critical infrastructure colleagues and partners to discuss the Microsoft Exchange Server vulnerabilities. Representatives from CISA, Microsoft, and Volexcity will discuss the vulnerabilities and highlight information that has been shared.

Date/Time: Friday, March 5, 2021 at 12:00pm EST
Participant Toll Free Dial in Number: 1-800-857-6546 (passcode 9975125)
International Dial in Number: 1-517-308-9490 (passcode 9975125)

Next Steps (if you maintain on-premises Microsoft Exchange Servers)

- Assume (and operate as) you have been compromised
- Address the alerts and patch immediately
- Externally validate the patch
- Look for the presence of the webshells and other IoCs (from the CISA
- Alert and other guidance, such as the Volexity and Huntress posts)

WaterISAC will continue to share information with its members and partners as more is learned, including via the "Microsoft Exchange Server Vulnerabilities: Information and Mitigation Resources" webpage on its portal. It urges members to report incidents and suspicious activities, first to local and other law enforcement authorities and then to WaterISAC by emailing analyst@waterisac.org, calling 866-H2O-ISAC, or using the online incident reporting form.

- The WaterISAC Team

TLP:GREEN

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

Read more about the Traffic Light Protocol (TLP) at the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

The international security network created by and for water sector professionals.

WaterISAC | 866-H2O-ISAC | info@waterisac.org | www.waterisac.org

1620 I Street NW
Suite 500
Washington, DC 20006
United States

From: WaterISAC <info@waterisac.org>
Sent: Wednesday, March 3, 2021 7:30 PM
Subject: UPDATE: CISA Releases Alert and Emergency Directive on Microsoft Exchange Server Vulnerabilities

WATER ISAC

SUPERCHARGE YOUR SECURITY

WaterISAC Members,

WaterISAC encourages members review and take action on two new products released by the Cybersecurity and Infrastructure Security Agency (CISA) regarding newly-disclosed vulnerabilities in on-premises Microsoft Exchange Servers. These products are in addition to the those listed in an advisory sent to members earlier today and include:

- Alert (AA21-062A): Mitigate Microsoft Exchange Server Vulnerabilities
- Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities

Alert

As noted in the alert, CISA's partners have observed active exploitation of these vulnerabilities. Successful exploitation of the vulnerabilities allows an unauthenticated attacker to execute arbitrary code on vulnerable Exchange Servers, as well as access files and mailboxes on the server and to credentials stored on that system. Additionally, the attacker may be able to compromise trust and identity in a vulnerable network. Microsoft released out-of-band patches to address the vulnerabilities, which are listed and described in the alert.

The alert also includes tactics, techniques and procedures (TTPs) and the indicators of compromise (IOCs), which CISA recommends organizations use to detect any malicious activity. If an organization discovers exploitation activity, they should assume network identity compromise and follow incident response procedures. If an organization finds no activity, they should apply available patches immediately and implement the mitigations in the alert.

Emergency Directive

The Emergency Directive applies to federal civilian agencies, but CISA encourages all organizations to read it and take appropriate steps to protect their networks. WaterISAC also recommends members review the Emergency Directive given the severity of the vulnerabilities. Non-federal civilian agencies have previously used CISA's Emergency Directives to inform their mitigation efforts, including during the response to the SolarWinds exploitation campaign. For that, WaterISAC joined with other sector stakeholders in encouraging water and wastewater utilities to use CISA's Emergency Directive.

Next Steps

WaterISAC will continue to share information with its members and partners as more is learned. It urges members to report incidents and suspicious activities, first to local and other law enforcement authorities and then to WaterISAC by emailing analyst@waterisac.org, calling 866-H2O-ISAC, or using the online incident reporting form.

- The WaterISAC Team

The international security network created by
and for water sector professionals.

WaterISAC | 866-H2O-ISAC | info@waterisac.org | www.waterisac.org

1620 I Street NW
Suite 500
Washington, DC 20006
United States