Hive Pro

THREAT ADVISORY

Old Zimbra vulnerability used to target Ukrainian Government Organizations

TA2022094

Threat Level AMBER

Publish Date – April 18, 2022

The Ukrainian Computer Emergency Response Team (CERT-UA) has issued an alert about a campaign targeting Ukrainian government entities that involves an exploit for an XSS vulnerability in Zimbra Collaboration Suite.

The attackers have been sending out phishing emails with the subject "Volodymyr Zelenskyy presented the Golden Star Orders to servicemen of the Armed Forces of Ukraine and members of the families of the fallen Heroes of Ukraine" which contain JavaScript code that evokes the exploitation of the vulnerability (CVE-2018-6882) in Zimbra Collaboration Suite, an email and collaboration platform.

The vulnerability is exploited in attacks to add a forwarding rule for the victim's emails to a new address under the attacker's control. This campaign is attributed to UAC-0097, a currently unknown threat actor, with moderate confidence.

The MITRE ATT&CK TTPs used by UAC-0097 are:
TA0001: Initial Access
T1566: Phishing
T1566.001: Phishing: Spearphishing Attachment
TA0002: Execution
T1204: User Execution
T1059: Command and Scripting Interpreter
T1059.007: Command and Scripting Interpreter: JavaScript

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2018-6882	Zimbra Collaboration Suite (ZCS) before 8.7 Patch 1 and 8.8.x before 8.8.7	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*	Cross-site scripting (XSS) vulnerability in the ZmMailMsgView.getAttachmentLinkHtml function	CWE-79

Patch Links

https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.7

References

https://cert-gov-ua.translate.goog/article/39606?_x_tr_sl=uk&_x_tr_tl=en&_x_tr_hl=de&_x_tr_pto=wapp