ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

CISCO Zero-Day Vulnerabilities Exploitation in Bangladesh

Date: 26 October 2023

Cyber Threat Advisory: CISCO Zero-Day Vulnerabilities Exploitation in Bangladesh

The Cyber Threat Intelligence Unit of BGD e-GOV CIRT warns about the ongoing exploitation of two zero-day vulnerabilities in Cisco's IOS XE Software web UI feature. BGD e-GOV CIRT has recently identified successful exploitation attempts against organizations in Bangladesh. This advisory is directed towards IT teams configuring and managing routers and network switches within their organizations.

1. **CVE-2023-20198** (Critical | CVSS: 10.0): Allows remote attackers to create local user accounts, posing a severe privilege escalation risk.

2. **CVE-2023-20273** (High | CVSS: 7.2): Chained with the first vulnerability, it facilitates elevated privileges and malicious implant injection.

Scope & Impact:

Affected Systems: All Cisco IOS XE Software with Web UI enabled.

Risk Level: Critical

Potential Impact: Network traffic monitoring, redirection, security breach, and implant injection by unauthorized intruders.

Recommendations

To determine if a device might be compromised, consider the following actions:

1. **Examine Log Messages:** Review system logs for specific log entries involving unfamiliar local users, including:

   %SYS-5-CONFIG_P: Configuration modifications made by certain processes as "user."

   %SEC_LOGIN-5-WEBLOGIN_SUCCESS: Records of successful web logins, including user and source IP details.

   %WEBUI-6-INSTALL_OPERATION_INFO: Instances of user-initiated installations for unknown filenames.

2. **Detect Malicious Implant:** Check for a malicious implant on potentially compromised Cisco IOS XE devices by running the command below. Replace "DEVICEIP" with the target device's IP address. Employ a generic curl command to identify systems hosting known implant variants without engaging the implant's primary functions. By using %25 (percent-encoded percent), you can trigger distinct responses. If the response contains a 404 HTTP error along with a "404 Not Found" message, it suggests a recognized implant variation. Systems without the implant will produce either the typical 404 HTTP response or a JavaScript redirect with a 200 HTTP response.

BGD e-GOV CIRT

If the implant is present, you will get a response similar to the following:

```
$ curl -k 'https://DEVICEIP/%25'
<html>
<head><title>404 Not
Found</title></head>
<body bgcolor="white">
<center><h1>404 Not
Found</h1></center>
<hr><center>nginx</center>
</body>
```

If the implant is **not** present, you will get a different response. For example:

```
$ curl -k 'https://DEVICEIP/%25'
<script>window.onload=function(){ url ='/webui';window.location.href=url;}</script>
```

Please note: When inspecting devices with insecure web interfaces, apply the HTTP scheme.

Indicators of Compromise

IPv4 Addresses	Usernames
5.149.249[.]74	cisco_tac_admin
154.53.56[.]231	cisco_support
154.53.63[.]93	cisco_sys_manager

Mitigations

Cisco has made available software updates to address the vulnerabilities outlined in this advisory. Additionally, it has indicated that customers with service agreements granting them access to routine software updates can acquire the necessary security patches through their standard update sources. Detailed information can be found in the Cisco advisory provided at the following link:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z