BrickerBot Permanent Denial-of-Service Attack (Update A)

ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

SUMMARY

This updated alert is a follow-up to the original alert titled ICS-ALERT-17-102-01A BrickerBot Permanent Denial-of-Service Attack that was published April 12, 2017, on the NCCIC/ICS-CERT web site.

ICS-CERT is aware of open-source reports of “BrickerBot” attacks, which exploit hard-coded passwords in IoT devices in order to cause a permanent denial of service (PDoS). This family of botnets, which consists of BrickerBot.1 and BrickerBot.2, was described in a Radware Attack Report (‘BrickerBot’ Results In PDoS Attack).

ICS-CERT is working to identify vendors of affected IoT devices in order to collect product-specific mitigations and compensating controls. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

DETAILS

--------- Begin Update A Part 1 of 2 --------

According to Radware, this bot attack is designed to render a connected device useless by causing a PDoS, or “bricked” state. BrickerBot.1 and BrickerBot.2 exploit hard-coded passwords, exposed SSH, and brute force Telnet. According to Radware’s Attack Report and open source reporting, the following details regarding BrickerBot.1 and BrickerBot.2 are available:

- BrickerBot.1 targets devices running BusyBox with an exposed Telnet command window. These devices also have SSH exposed through an older version of Dropbear SSH server. Most of these devices were also identified as Ubquiti network devices running outdated firmware. Some of these devices are access points or bridges with beam directivity. BrickerBot.1 was active from March 20, 2017 to March 25, 2017. According to Radware, BrickerBot.1 attacks have ceased.
- BrickerBot.2 targets Linux-based devices which may or may not run BusyBox and which expose a Telnet service protected by default or hard-coded passwords. The source of the attacks is concealed by TOR exit nodes.
- No information is available at this time about the type and number of devices used in performing these attacks.

--------- End Update A Part 1 of 2----------

This situation is still developing. ICS-CERT is working to identify vendors of affected devices in order to collect more detailed mitigation information.

MITIGATION

ICS-CERT is currently working to identify vendors of affected IoT devices in order to collect more detailed mitigation information. Radware recommended taking the following precautions in the Attack Report above:

- Change the device's factory default credentials.
- Disable Telnet access to the device.
- Use network behavioral analysis to detect anomalies in traffic and combine with automatic signature generation for protection.
- Set intrusion protection systems to block Telnet default credentials or reset telnet connections. Use a signature to detect the provided command sequences.

--------- Begin Update A Part 2 of 2 --------

Update your Ubiquiti Networks devices with the latest firmware.

--------- End Update A Part 2 of 2----------

Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

ICS-CERT strongly encourages asset owners not to assume that their control systems are deployed securely or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities. Control systems often have Internet accessible devices installed without the owner's knowledge, putting those systems at increased risk of attack.

ICS-CERT recommends, as quality assurance, that users test the mitigations in a test development environment that reflects their production environment prior to installation. In addition, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Remove, disable, or rename any default system accounts wherever possible.
- Apply patches in the ICS environment, when possible to mitigate known vulnerabilities.
- Implement policies requiring the use of strong passwords.
- Monitor the creation of administrator level accounts by third-party vendors.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT also provides a control systems recommended practices page on the ICS-CERT web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870
For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.