Log In or Sign Up (/ExtrLogin?startURL=%2Fextrarticledetail)

Search

Updated July 2026
The ExtremeCloud IQ classic UI retirement has been updated to Q2, Calendar Year 2027. After that, only the new UI will be available. No customer action is required. For more details based on the platform you use today, please see the links below:
ExtremeCloud IQ (https://community.extremenetworks.com/t5/extremecloud-iq-xiq/extremecloud-iq-ui-transition-what-you-need-to-know/ba-p/121452#M54) **Extreme Platform ONE (https://community.extremenetworks.com/t5/extreme-platform-one-networking/extremecloud-iq-ui-transition-what-extreme-platform-one-users/td-p/121451)**

SA-2023-135 - IQ Engine ah_bgd service buffer overflow (CVE-2023-46273)

Create Case (/ExtrCaseCreation)

Article Type: Security Advisory
Article Number: 000115356
Last Modified: 12/5/2023

Summary

The IQ Engine Bonjour Gateway daemon contains has a stack-based buffer overflow that allows an attacker to call the 'ah_event_send' function with a crafted 'event_id' and 'event_message', targeting the 'ah_scd' daemon which is also vulnerable to a stack-based buffer overflow, allowing an attacker to execute arbitrary code as root.

Extreme Networks acknowledges and thanks Victorien Molle (biche@biche.re) for reporting this vulnerability to Extreme under coordinated vulnerability disclosure protocols.

Products not listed in the Impact Details section have not been evaluated. Furthermore, products that have exceeded any software maintenance time periods are also not evaluated and will not be published. Please consult End of Sale and End of Service Life - Extreme Networks (https://www.extremenetworks.com/support/end-of-sale-and-end-of-support-products/) for the EOL notices related to the product under question.

Products Potentially Affected

Impact Details

OS/Product	Exposure
IQ Engine (HiveOS)	Yes

Repair Recommendations

IQ Engine (HiveOS):

- Fixed in 10.6r1a or later:
  AP30
  AP122
  AP122X
  AP130
  AP150W
  AP230
  AP245X
  AP250
  AP550
  AP1130

- Fixed in 10.6r5 or later:
  AP302W
  AP305C/CX
  AP305C-1
  AP410C
  AP410C-1
  AP460C
  AP460S6C
  AP460S12C
  AP510C/CX
  AP630
  AP650
  AP650X
  AP3000
  AP3000X
  AP4000
  AP4000-1
  AP5010
  AP5050D
  AP5050U

Legal Notice

This advisory notice is provided on an “as is” basis and Extreme Networks makes no representations or warranties of any kind, expressly disclaiming the warranties of merchantability or fitness for a particular use. Use of the information provided herein or materials linked from this advisory notice is at your own risk. Extreme Networks reserves the right to change or update this document at any time, and expects to update this document as new information becomes available. The information provided herein is applicable to current Extreme Networks products identified herein and is not intended to be any representation of future functionality or compatibility with any third-party technologies referenced herein. This notice shall not change any contract or agreement that you have entered into with Extreme Networks.

Version

1

Related Content

- SA-2023-134 - IQ Engine ah_auth buffer overflow (CVE-2023-46272) (/ExtrArticleDetail?an=000115355)
- Where can I Download Latest Software and Firmware Releases for my Extreme Products? (/ExtrArticleDetail?an=000083342)
- FN-2025-510 - Removal of Switch Engine and Summit EXOS Software Releases from Extreme Portal (/ExtrArticleDetail?an=000122602)
- SA-2026-151 - GNU Wget Buffer Overflow src url.c (CVE-2026-58471) (/ExtrArticleDetail?an=000138477)
- SA-2026-095 - UAF in xmlParseInternalSubset (CVE-2026-6653) (/ExtrArticleDetail?an=000138471)

Ask the Hub
(https://community.extremenetworks.com)

Feedback

If you would like to receive a response regarding your feedback, please log in to the Support Portal

Was this article helpful in resolving your issue?

© 2026 Extreme Networks, Inc. All rights reserved.