



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

January 25, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2016-017

DATE(S) ISSUED:

01/25/2016

SUBJECT:

Vulnerability in AMX Harman Professional Devices Could Allow Unauthorized Remote Access

OVERVIEW:

A vulnerability has been discovered in AMX Harman Professional devices that could allow full unauthorized remote access. AMX Harman Professional devices are audio-visual (AV) products focused on solving the complexity of managing technology with reliable, consistent and scalable systems comprising control and automation, system-wide switching and AV signal distribution, digital signage and technology management. Successful exploitation could grant the attacker full control over the impacted AMX device.

THREAT INTELLIGENCE:

Even though the backdoor usernames are available on the Internet, there are currently no reports of the vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

Including but not limited to:

- AMX NX-1200
- AMX DGX16-ENC (Digital Media Switchers)
- AMX DGX32-ENC-A (Digital Media Switchers)
- AMX DGX64-ENC (Digital Media Switchers)
- AMX DGX8-ENC (Digital Media Switchers)
- AMX DVX-2100HD (All-In-One Presentation Switchers)
- AMX DVX-2210HD (All-In-One Presentation Switchers)
- AMX DVX-2250HD (All-In-One Presentation Switchers)
- AMX DVX-2255HD (All-In-One Presentation Switchers)
- AMX DVX-3250HD (All-In-One Presentation Switchers)
- AMX DVX-3255HD (All-In-One Presentation Switchers)
- AMX DVX-3256HD (All-In-One Presentation Switchers)
- AMX ENOVADGX64-ENC (Digital Media Switchers)
- AMX MCP-106 (ControlPads)
- AMX MCP-108 (ControlPads)
- AMX NI-2000 (Central Controllers)
- AMX NI-2100 (Central Controllers)
- AMX NI-3000 (Central Controllers)
- AMX NI-3100 (Central Controllers)
- AMX NI-3101-SIG (Central Controllers)
- AMX NI-4000 (Central Controllers)
- AMX NI-4100 (Central Controllers)
- AMX NI-700 (Central Controllers)
- AMX NI-900 (Central Controllers)
- AMX NX-1200 (Central Controllers)
- AMX NX-2200 (Central Controllers)
- AMX NX-3200 (Central Controllers)
- AMX NX-4200 (Central Controllers)
- AMX NXC-ME260-64 (Central Controllers)
- AMX NXC-MPE (Central Controllers)
- AMX NetLinx NX Integrated Controller (Media)

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A**TECHNICAL SUMMARY:**

A vulnerability has been discovered in AMX Harman Professional devices that could allow full unauthorized remote access. The vulnerability identified could provide an attacker with full control of a vulnerable AMX device. The usernames "1MB@tMaN" and "BlackWidow" were hard-coded in the firmware and allow for remote login in debug mode, granting the attacker access to tools not provided to administrators such as packet sniffing. AMX has released patches to fix the issue for some of the affected devices.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the updates provided by AMX immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred before applying the patch.
- Monitor logs for signs of access by either of these accounts.
- Unless required, limit external network access to affected products.

REFERENCES:**CERT-SEI:**

<https://www.kb.cert.org/vuls/id/992624>

AMX:

<http://www.amx.com/techcenter/NXSecurityBrief/>

Sec-Lists:

<http://seclists.org/fulldisclosure/2016/Jan/63>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8362>

Sec Consult:

<http://blog.sec-consult.com/2016/01/deliberately-hidden-backdoor-account-in.html>