

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

01/25/2016

**02/19/2016 – UPDATED**

**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)

**February 19 - UPDATED SYSTEM AFFECTED:**

- ***NX-1200, NX-2200, NX-3200, NX-4200 NetLinx Controller, versions prior to Version 1.4.65***
- ***Massio ControlPads MCP-10x, versions prior to Version 1.4.65***
- ***Enova DVX-x2xx, versions prior to Version 1.4.65***
- ***DVX-31xxHD-SP (-T), versions prior Version 4.8.331***
- ***DVX-21xxHD-SP (-T), versions prior Version 4.8.331***
- ***DVX-2100HD-SP-T Master, versions prior to Version 4.1.420 (Hotfix firmware version)***
- ***Enova DGX 100 NX Series Master, versions prior to Version 1.4.72 (Hotfix firmware version)***
- ***Enova DGX 8/16/32/64 NX Series Master, versions prior to Version 1.4.72 (Hotfix firmware version)***
- ***Enova DGX 8/16/32/64 NI Series Master, versions prior to Version 4.2.397 (Hotfix firmware version)***
- ***NI-700, NI-900 Master Controllers (64M RAM), versions prior to Version 4.1.419***
- ***NI-700, NI-900 Master Controllers (32M RAM), versions prior to Version 3.60.456 (Hotfix firmware version)***
- ***NI-2100, NI-3100, NI-4100, NI-2100 with ICSNet, NI-3100 with ICSNet, NI-3100/256***
- ***NI-3100/256 with ICSNet, NI-4100/256, versions prior to Version 4.1.419***
- ***NI-3101-SIG Master Controller, versions prior to Version 4.1.419***
- ***NI-2000, NI-3000, NI-4000, versions prior to Version 3.60.456 (Hotfix firmware version), and***
- ***ME260/64 Duet, versions prior to Version 3.60.456 (Hotfix firmware version).***
- ***NX-1200, NX-2200, NX-3200, NX-4200 NetLinx Controller, Version 1.4.65 and Version 1.4.66 (Hotfix firmware version)***
- ***Massio ControlPads MCP-10x, Version 1.4.65 and Version 1.4.66 (Hotfix firmware version)***
- ***Enova DVX-x2xx, Version 1.4.65 and Version 1.4.72 (Hotfix firmware version)***
- ***Enova DGX 100 NX Series Master, Version 1.4.72 (Hotfix firmware version)***
- ***Enova DGX 8/16/32/64 NX Series Master, Version 1.4.72 (Hotfix firmware version)***

**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:**

The following actions should 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.

**February 19 – UPDATED RECOMMENDATIONS:**

**Updates for CVE-2016-1984 are not scheduled to be released until April 2016. Until then, consider the following mitigation techniques:**

- ***If there are no ICSP devices connected via the external interface, disable the ICSP protocol.***
- ***Isolate affected systems from external and untrusted networks and hosts.***

**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>

**February 19 – Updated References:****CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1984>

TLP: WHITE

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction,  
subject to copyright controls.  
<http://www.us-cert.gov/tlp/>**