VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2018-006
CVE ID: CVE-2018-18244, CVE-2018-18005, CVE-2018-18004
First Published: December 28, 2018
Last Update: December 28, 2018
Status: Fixed
Revision: 1

Overview:

Security researcher Paul Yun of Independent Security Evaluators discovered the following vulnerability.

CVE-2018-18244, affected firmware 0x06x to 0x08x, have persistent XSS vulnerability via HTTP referer header.

CVE-2018-18005, affected firmware 0x06x to 0x08x, have DOM-Based XSS vulnerability via event_script.html.

CVE-2018-18004, when internal debug mode (telnet service) is enabled, web UI will not show any warning message to client.

Affect Products:

All Network Camera Series.

Workarounds:

None.

Solution:

Please upgrade firmware to XXXXXX-VVTK-0X09a or above.

Revision History:

Revision 1 / December 28, 2018 / Initial release