Are Hirschmann Classic Switches affected by the VxWorks vulnerabilities described in CVE-2019-12256, CVE-2019-12257, CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263, CVE-2019-12258, CVE-2019-12259, CVE-2019-12262, CVE-2019-12264, CVE-2019-1

Christoph Wrobel - 2019-08-15 - Classic Switches

Hirschmann Classic Switches are NOT affected by the VxWorks vulnerabilities described in CVE-2019-12256, CVE-2019-12257, CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263, CVE-2019-12258, CVE-2019-12259, CVE-2019-12262, CVE-2019-12264, CVE-2019-12265.

Hirschmann devices belonging to "Classic Switches" are e.g.:
- RS20..., RS30..., RS40...,
- RSR...
- MACH1000, MACH4002

Classic Switches use firmware packets marked as L2E, L2P, L3E, L3P

Please note that the Product Families DRAGON MACH, RSP, RSPE belong to the HiOS product group and use a different operating system.

Generally Hirschmann recommend to **always use the latest firmware version** if not explicitely advised differently.

Tags

CVE-2019-12255
CVE-2019-12256
CVE-2019-12257
CVE-2019-12258
CVE-2019-12259
CVE-2019-12260
CVE-2019-12261
CVE-2019-12262
CVE-2019-12263

CVE-2019-12264

CVE-2019-12265

VxWorks