

Receive Security Alerts

[Subscribe](#) to our mailing list to receive updates regarding new security advisories.

Security Advisories

Last Update: April 2nd, 2026

✕

We use necessary cookies to make our site work. By clicking "accept all" you agree that we may also set optional analytics and third party behavioral advertising cookies to help us improve our site and to share certain information with third parties. For more information on how these cookies work, please see our [Cookie Consent Policy](#).

[Manage Preferences](#)
[Reject All Cookies](#)
[Accept All Cookies](#)

Identifier				Document Download
PSIRT-5	OpenSSL Vulnerabilities in NRSW	1.0	2026-04-02	Security Advisory
PSIRT-3	RADIUS Protocol under RFC 2865 is susceptible to forgery attacks	1.2	2026-03-13	Security Advisory
PSIRT-4	MongoDB Vulnerability in Connectivity Suite	1.0	2026-01-21	Security Advisory
PSIRT-2	Web Interface Vulnerability in HiOS	1.0	2025-10-10	Security Advisory
BSECV-2024-16	Web interface vulnerability in HiLCOS	1.0	10.16.2024	Security Bulletin
BSECV-2023-05	Multiple OpenSSL vulnerabilities in Hirschmann products	1.1	06.25.2024	Security Bulletin
BSECV-2022-17	Multiple BusyBox vulnerabilities in BAT-C2 and OWL	1.0	05.13.2024	Security Bulletin
BSECV-2024-02	Web Server Authentication Bypass Vulnerability in HiEOS	1.0	04.26.2024	Security Bulletin
BSECV-2022-07	Multiple expat vulnerabilities in Hirschmann HiOS/ HiSecOS, BAT-C2 & GECKO products.	1.0	09.27.2023	Security Bulletin
BSECV-2022-30	Zlib has a heap-based buffer over-read or buffer overflow	1.0	8.8.2023	Security Bulletin
BSECV-2021-15	Multiple NTP vulnerabilities in HiSecOS	1.0	07.25.2023	Security Bulletin
BSECV-2021-27	DNS request vulnerability in Firewall Products	1.0	07.25.2023	Security Bulletin
BSECV-2022-16	net-snmp vulnerability in Hirschmann HiSecOS	1.0	07.25.2023	Security Bulletin
BSECV-2023-10	Java SE vulnerability in Belden/Hirschmann software products	1.0	07.17.2023	Security Bulletin

Identifier	Document Title	Version	Last Updated	Document Download
BSECV-2022-26	Multiple libexpat vulnerabilities in HiOS, Classic, HiSecOS, Wireless BAT-C2, Lite Managed.	1.0	04.25.2023	Security Bulletin
BSECV-2022-29	<p>We use necessary cookies to make our site work. By clicking “accept all” you agree that we may also set optional analytics and third party behavioral advertising cookies to help us improve our site and to share certain information with third parties. For more information on how these cookies work, please see our Cookie Consent Policy.</p>			Security Bulletin
BSECV-2023-06				Security Bulletin
	arbitrary scripts or binaries			
BSECV-2021-07	HiSecOS Web Server Vulnerability Allows User Role Privilege Escalation	1.0	01.30.2023	Security Bulletin
BSECV-2022-18	Multiple vulnerabilities in BAT-C2	1.0	11.23.2022	Security Bulletin
BSECV-2022-21	Authenticated Command Injection in Hirschmann BAT-C2	1.0	11.23.2022	Security Bulletin
BSECV-2022-20	TinyXML vulnerability in Hirschmann HiLCOS products	1.0	11.23.2022	Security Bulletin
BSECV-2022-12	Multiple Java SE vulnerabilities in Belden/Hirschmann software products	1.0	11.10.2022	Security Bulletin
BSECV-2021-03	Industrial HiVision: Configured external applications may result in execution of arbitrary binaries	1.0	10.17.2022	Security Bulletin
BSECV-2022-13	Denial of Service Vulnerability in EagleSDV	1.0	08.01.2022	Security Bulletin
BSECV-2021-16	FragAttacks Hirschmann BAT	1.1	08.01.2022	Security Bulletin
BSECV-2022-09	FragAttacks ProSoft RadioLinx RLX2	1.0	07.01.2022	Security Bulletin
BSECV-2022-11	Multiple vulnerabilities in Provize Basic Frontend	1.0	05.03.2022	Security Bulletin
BSECV-2022-05	Multiple vulnerabilities in Provize Basic Backend	1.0	05.03.2022	Security Bulletin
BSECV-2022-01	Vulnerability in ‘axios’ HTTP client in Provize Basic	1.0	05.03.2022	Security Bulletin
BSECV-2021-05	Multiple Vulnerabilities in Tofino	1.1	01.11.2022	Security Bulletin
BSECV-2020-03	Potential denial of service vulnerability in PROFINET Devices via DCE-RPC Packets	1.0	10.21.2021	Security Bulletin

Identifier	Document Title	Version	Last Updated	Document Download
BSECV-2020-10	Password Change Authentication Bypass Vulnerability in HiOS & HiSecOS	1.0	05.11.2021	Security Bulletin
BSECV-2019-08	<p>We use necessary cookies to make our site work. By clicking "accept all" you agree that we may also set optional analytics and third party behavioral advertising cookies to help us improve our site and to share certain information with third parties. For more information on how these cookies work, please see our Cookie Consent Policy.</p>			Security Bulletin
BSECV-2021-02				Security Bulletin
BSECV-2019-09				IPsec Firewall Bypass Vulnerability in WLAN (HiLCOS) Products
BSECV-2020-08	EtherNet/IP Vulnerability in 2012 release of (3) PLX31s	1.0	12.18.2020	Security Bulletin
BSECV-2019-14	HiOS EtherNet/IP stack vulnerability	1.0	09.09.2020	Security Bulletin
BSECV-2020-04	Multiple dnsmasq Vulnerabilities in OWL 3G, LTE & LTE M12	1.0	06.15.2020	Security Bulletin
BSECV-2020-02	JAVA SE vulnerability in Industrial HiVision	1.0	06.15.2020	Security Bulletin
BSECV-2020-06	pppd vulnerability in Hirschmann OWL Devices	1.0	5.28.2020	Security Bulletin
BSECV-2020-01	Web Server Buffer Overflow in HiOS & HiSecOS products	1.2	03.25.2020	Security Bulletin
BSECV-2019-05	Multiple IP vulnerabilities in Hirschmann HiOS and Classic Firewall and GarrettCom DX products (URGENT/11)	1.3	11.27.2019	Security Bulletin
BSECV-2018-06	Belden GarrettCom MNS 6K and 10K OpenSSL Vulnerabilities	1.0	08.09.2019	Security Bulletin
BSECV-2018-08	Belden GarrettCom MNS 6K and 10K SNMP Vulnerability	1.0	08.09.2019	Security Bulletin
BSECV-2018-07	Jackson vulnerability in Industrial HiVision	1.0	06.06.2018	Security Bulletin
BSECV-2017-11	strongSwan vulnerability in HiSecOS	1.0	06.06.2018	Security Bulletin
BSECV-2017-16	WPA2 Key Reinstallation Attack (KRACK) vulnerabilities in Hirschmann BAT devices	1.1	06.06.2018	Security Bulletin
BSECV-2017-15	Web Server Authentication Bypass Vulnerability in HiOS & HiSecOS	1.0	05.25.2018	Security Bulletin

Identifier	Document Title	Version	Last Updated	Document Download
BSECV-2018-02	Weaknesses in Hirschmann Classic Platform Switches when using plaintext HTTP for remote management	1.1	03.09.2018	
BSECV-2018-03	<p>We use necessary cookies to make our site work. By clicking "accept all" you agree that we may also set optional analytics and third party behavioral advertising cookies to help us improve our site and to share certain information with third parties. For more information on how these cookies work, please see our Cookie Consent Policy.</p>			Security Bulletin
BSECV-2018-04				Security Bulletin
BSECV-2017-14; CVE-2017-11400; CVE-2017-11401; CVE-2017-11402	Potential Tofino Firmware Signing / Protocol Filtering Evasion / Firewall Bypass	1.0	11.06.2017	Security Bulletin
BSECV-2017-2	Unauthenticated remote code execution vulnerability in Industrial HiVision	1.0	08.18.2017	Security Bulletin
BSECV-2017-12	Vulnerability in the bundled Java Runtime Environment lets local users execute arbitrary code in Industrial HiVision, HiFusion and HiView	1.0	08.11.2017	Security Bulletin
BSECV-2017-10	ICX35 User Interface Input Validation Issue	1.0	05.08.2017	Security Bulletin
BSECV-2017-9	ICX35 Authentication Vulnerability	1.0	05.08.2017	Security Bulletin
BSECV-2017-8	Belden GarrettCom MNS 6K and 10K Device Access and Security Key Vulnerabilities	1.0	05.08.2017	Security Bulletin
BSECV-2017-3	Potential false forward of IPv4 multicast/broadcast traffic by HiLCOS Layer-2 Firewall	1.0	05.08.2017	Security Bulletin
BSECV-2017-7	Possible Request Forgery Vulnerabilities for GECKO Devices	1.0	04.07.2017	Security Bulletin
BSECV-2017-1	Restricted user roles may gain write access to devices managed by Industrial HiVision	1.0	01.06.2017	Security Bulletin
BSECV-2016-2	Passwords Synchronization with SNMP v1/v2 communities	1.1	12.19.2016	Security Bulletin
BSECV-2016-5	Possible Information Disclosure for GECKO Devices	1.0	12.19.2016	Security Bulletin
BSECV-2016-4	HiOS TCP Initial Sequence Number Predictability	1.0	06.06.2016	Security Bulletin

Identifier	Document Title	Version	Last Updated	Document Download
BSECV-2016-1	GECKO authentication bypass	1.0	03.07.2016	Security Bulletin
BSECV-2015-5	Identical SSH and SSL			Security Bulletin
BSECV-2015-4;CVE-2008-0960				Security Bulletin

We use necessary cookies to make our site work. By clicking "accept all" you agree that we may also set optional analytics and third party behavioral advertising cookies to help us improve our site and to share certain information with third parties. For more information on how these cookies work, please see our [Cookie Consent Policy](#).