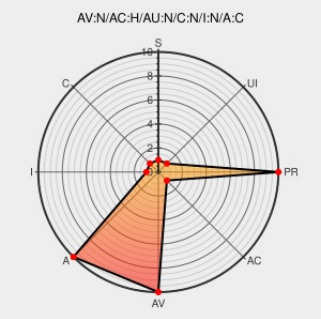
CVE-2006-5179

Published on: 10/05/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:02 PM UTC

CVE-2006-5179

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Igateway Ssl-vpn from Intoto contain the following vulnerability:

Intoto iGateway VPN and iGateway SSL-VPN allow context-dependent attackers to cause a denial of service (CPU consumption) via parasitic public keys with large (1) "public exponent" or (2) "public modulus" values in X.509 certificates that require extra time to process when using RSA signature verification, a related issue to CVE-2006-2940.

CVE-2006-5179 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
	Vendor Advisory, www.uniras.gov.uk, application/pdf, Inactive Link, Not Archived	MISC www.uniras.gov.uk/niscc/docs/re-20060928-00661.pdf?lang=en
Intoto iGateway VPN / SSL-VPN Denial of Service Vulnerability - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 22206
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com, text/html	VUPEN ADV-2006-3859

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Intoto	Igateway Ssl-vpn	All	All	All	All
Hardware	Intoto	Igateway Ssl-vpn	All	All	All	All
Hardware	Intoto	Igateway Vpn	All	All	All	All
Hardware	Intoto	Igateway Vpn	All	All	All	All

cpe:2.3:h:intoto:igateway_ssl-vpn:*:*:*:*:*:*:*:*:

cpe:2.3:h:intoto:igateway_ssl-vpn:*:*:*:*:*:*:*:*:

cpe:2.3:h:intoto:igateway_vpn:*:*:*:*:*:*:*:*:

cpe:2.3:h:intoto:igateway_vpn:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→