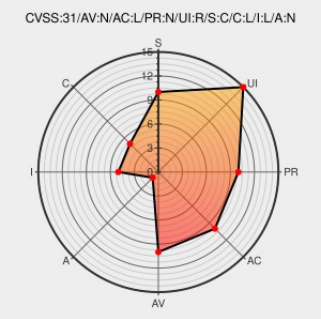
CVE-2017-9037

Published on: 05/25/2017 12:00:00 AM UTC

Last Modified on: 09/09/2021 05:33:00 PM UTC

CVE-2017-9037

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



Certain versions of Serverprotect from Trendmicro contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in Trend Micro ServerProtect for Linux 3.0 before CP 1531 allow remote attackers to inject arbitrary web script or HTML via the (1) S44, (2) S5, (3) S_action_fail, (4) S_ptn_update, (5) T113, (6) T114, (7) T115, (8) T117117, (9) T118, (10) T_action_fail, (11) T_ptn_update, (12) textarea, (13) textfield5, or (14) tmLastConfigFileModifiedDate parameter to notification.cgi.

CVE-2017-9037 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Trend Micro ServerProtect Disclosure / CSRF / XSS ≈ Packet Storm	Exploit, Third Party Advisory	MISC packetstormsecurity.com/files/142645/Trend-

	VDB Entry packetstormsecurity.com text/html	Micro-ServerProtect-Disclosure-CSRF-XSS.html
Full Disclosure: [CORE-2017-0002] - Trend Micro ServerProtect Multiple Vulnerabilities	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20170523 [CORE-2017-0002] - Trend Micro ServerProtect Multiple Vulnerabilities
Multiple Vulnerabilities - ServerProtect for Linux 3.0	Patch Vendor Advisory success.trendmicro.com text/html	CONFIRM success.trendmicro.com/solution/1117411
Trend Micro ServerProtect for Linux Multiple Bugs Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting and Cross-Site Request Forgery Attacks and Let Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1038548
Trend Micro ServerProtect Multiple Vulnerabilities | Core Security	Exploit Technical Description Third Party Advisory www.coresecurity.com text/html	MISC www.coresecurity.com/advisories/trend-micro-serverprotect-multiple-vulnerabilities

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Serverprotect	3.0	All	All	All
Application	Trendmicro	Serverprotect	3.0	All	All	All
Application	Trendmicro	Serverprotect	3.0	All	All	All

cpe:2.3:a:trendmicro:serverprotect:3.0:*:*:*:*:linux:*:*:

cpe:2.3:a:trendmicro:serverprotect:3.0:*:*:*:*:linux_kernel:*:*:

cpe:2.3:a:trendmicro:serverprotect:3.0:*:*:*:*:linux_kernel:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report