



CVE-2018-6940

Published on: 02/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-6940

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Nat32](#) from [Nat32](#) contain the following vulnerability:

A `/shell?cmd=` XSS issue exists in the HTTPD component of NAT32 v2.2 Build 22284 devices that can be exploited for Remote Code Execution in conjunction with CSRF.

CVE-2018-6940 has been assigned by [M](#) [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
NAT32 2.2 Build 22284 - Remote Command Execution - Windows webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept	EXPLOIT-DB 44033

text/html

NAT32 Build 22284 Remote Command Execution
≈ Packet Storm

Exploit

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

📄

MISC packetstormsecurity.com/files/146373/NAT32-Build-22284-Remote-Command-Execution.html

Exploit

Third Party Advisory

hyp3rlinx.altervista.org

text/plain

📄

MISC hyp3rlinx.altervista.org/advisories/NAT32-REMOTE-COMMAND-EXECUTION-CVE-2018-6940.txt

SecurityFocus

www.securityfocus.com

text/html

🌐

BUGTRAQ 20180214 NAT32 Build (22284) Remote Code Execution CVE-2018-6940 (hyp3rlinx / apparition security)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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
Application	Nat32	Nat32	2.2	All	All	All
Application	Nat32	Nat32	2.2	All	All	All

cpe:2.3:a:nat32:nat32:2.2:*:*:*:*:*:

cpe:2.3:a:nat32:nat32:2.2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→